Sun Java System Communications Services 6 2005Q4 Delegated Administrator 管理ガイド

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–4103
2005 年 10 月

060125@13215

目次

表目次

図目次

はじめに

このマニュアルは、Sun ™Sun Java System Communications Services Delegated Administrator の設定方法と管理方法について説明しています。また Delegated Administrator のコマンドを、構文と例を示して説明します。

Delegated Administrator は、Sun Java System Messaging Server と Sun Java System Calendar Server のユーザー、グループ、ドメイン、リソースを Sun Java System Access Manager を使用してプロビジョニングするためのコンソール (グラフィカルユーザーインタフェース) とコマンド行ツールセットです。

この章では、次の項目について説明します。

対象読者

このマニュアルは、管理するサイトで、Delegated Administrator の管理、設定、配備を行う責任者を対象としています。

お読みになる前に

このマニュアルは、ソフトウェアの管理に関する責任者を対象とし、次の一般的な知識を持っていることを前提にしています。

- インターネットおよび WWW (ワールドワイドウェブ)
- Messaging Server のプロトコル
- Sun Java System 管理サーバー
- Sun Java System Directory Server および LDAP
- Sun Java System のコンソール
- 次のプラットフォームのシステム管理とネットワーキング
  - SPARC/x86 版 Solaris 8
  - SPARC/x86 版 Solaris 9
  - SPARC/x86 版 Solaris 10
  - HP-UX 11.x
  - Windows 2000

  一般的な配備アーキテクチャー

このマニュアルの構成

このマニュアルの内容を、次の表にまとめています。

表 **P–1** このマニュアルの構成

章	説明
第 1 章	ディレクトリ構成、管理者のロール、Delegated Administrator で提供されるサービスパッケージについて説明します。
第 2 章	Sun Java System Communications Services Delegated Administrator のインストールおよび設定に必要な手順を説明します。
第 3 章	Delegated Administrator の設定プログラムについて説明し、その設定手順を具体的に示します。
第 4 章	コンソールの外観の変更など、Delegated Administrator をカスタマイズする方法を説明します。

表 P–1 このマニュアルの構成　(続き)

章	説明
第 5 章	commadmin ユーティリティーを、構文と例を示して説明します。
付録 A	サービスプロバイダ管理者 (Service Provider Administrator) のロールと、サービスプロバイダ管理者で管理されるプロバイダ組織とビジネス組織について説明します。
付録 B	個々のコマンド行オプションについて属性値とタイムゾーン値を示します。
付録 C	Delegated Administrator をデバッグするときに調査するログファイルを示します。
付録 D	Delegated Administrator のパフォーマンスを向上させるための Delegated Administrator、Web コンテナ、および Directory Server のチューニングに関するヒントを示します。
付録 E	ACI を統合する方法と、使用されていない ACI をディレクトリから削除する方法について説明します。

関連マニュアル

Sun テクニカルマニュアルには、Web サイト http://docs.sun.com SM からオンラインでアクセスできます。アーカイブを参照したり、特定の書名や主題を検索したりすることができます。

Messaging Server のマニュアル

次の URL を使用すると、Messaging Server のすべてのマニュアルを参照できます。

http://docs.sun.com/coll/1312.1

次の文書が利用できます。

- 『Sun Java™System Messaging Server 管理ガイド』
- 『Sun Java™ System Messaging Server Administration Reference』
- 『Sun Java™ System Messaging Server MTA Developer's Reference』
- 『Sun Java™ System Messenger Express Customization Guide』

Messaging Server 製品群には、Sun Java™ System Directory Server や Administration Server などの製品も含まれています。これらの製品およびその他の製品のマニュアルは、次の URL で参照できます。

http://docs.sun.com/db/prod/sunone

ソフトウェアマニュアル以外に、Messaging Server ソフトウェアフォーラムで、特定の Messaging Server 製品に関する質問について、技術的なヘルプを参照してください。フォーラムには、次の URL をご利用ください。

http://swforum.sun.com/jive/forum.jsp?forum=15

Calendar Server のマニュアル

Calendar Server の全マニュアルについては、次の URL を参照してください。

http://docs.sun.com/coll/1313.1

次の文書が利用できます。

- 『Sun Java™ System Calendar Server 管理ガイド』
- 『Sun Java™ System Calendar Server Developer's Guide』

Communications Services のマニュアル

Communications Services の全製品に使用されるマニュアルについては、次の URL のいずれかを参照してください。

http://docs.sun.com/coll/1312.1

または

http://docs.sun.com/coll/1313.1

次の文書が利用できます。

- 『Sun Java™ System Communications Services リリースノート』
- 『Sun Java™ System Communications Services Delegated Administrator 管理ガイド』
- 『Sun Java™ System Communications Services 配備計画ガイド』
- 『Sun Java™ System Communications Services Schema Migration Guide』
- 『Sun Java™ System Communications Services Schema Reference』
- 『Sun Java™ System Communications Services Event Notification Service Guide』
- 『Sun Java™ System Communications Express 管理ガイド』
- 『Sun Java™ System Communications Express Customization Guide』

関連するサードパーティーの Web サイト

このマニュアルに掲載されているサードパーティーの URL を参照すると、追加および関連情報を入手できます。

注 – このマニュアル内で述べられるサードパーティーの Web サイトが、現在利用できるかどうかについて Sun は責任を負いません。こうしたサイトやリソース上またはこれらを通じて利用できるコンテンツ、広告、製品、その他の資料について Sun は推奨しているわけではなく、Sun はいかなる責任も負いません。また、このようなサイトやリソース上で、またはサイトやリソースを通じて利用できるコンテンツ、製品、サービスの使用または依存を原因として、または使用や依存に関連して生じた、または生じた疑いのある実際の損傷や損失、あるいは損傷や損失の疑いのあるものに対して Sun は責任を負いません。

マニュアル、サポート、およびトレーニング

Sun のサービス	**URL**	説明
マニュアル	`http://www.sun.com/documentation/`	PDF 文書および HTML 文書をダウンロードできます。また印刷マニュアルを注文できます
サポートおよびトレーニング	`http://www.sun.com/supportraining/`	技術サポート、パッチのダウンロード、および Sun のトレーニングコース情報を提供します

Sun のリソースへのオンラインアクセス

製品のダウンロード、プロフェッショナルサービス、パッチとサポート、開発者用の補足情報については、次の URL を参照してください。

- Download Center `http://wwws.sun.com/software/download/`
- プロフェッショナルサービス
  `http://www.sun.com/service/sunps/sunone/index.html`
- Sun Enterprise Services、Solaris パッチ、サポート
  `http://sunsolve.sun.com/`
- 開発用の情報 `http://developers.sun.com/prodtech/index.html`

Sun 技術サポートの連絡先

製品マニュアルで解決されない本製品に関する技術的な疑問点があれば、URL `http://www.sun.com/service/contacting` を参照してください。

表記上の規則

次の表に、このマニュアルで使用される表記上の変更点を示します。

表 **P–2** 表記上の規則

字体または記号	意味	例
`AaBbCc123`	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力	`.login` ファイルを編集します。 `ls -a` を使用して、すべてのファイルを表示します。 `machine_name% you have mail.`
`AaBbCc123`	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して示します	`machine_name%` **`su`** `Password:`

表 **P–2** 表記上の規則　　*(続き)*

字体または記号	意味	例
aabbcc123	変数を示します。実際に使用する特定の名前または値で置き換えます。	ファイルを削除するには、`rm` *filename* と入力します。
AaBbCc123	参照する書名、新しい単語、または、 強調する単語を示します。	『ユーザーズガイド』の第 6 章を参照してください。 パッチの分析を実行してください。 このファイルは保存しないでください。 （オンライン表示の場合、強調する語が太字で表示される場合があります。）

コマンド例で使用されるシェルプロンプト

次の表は、C シェル、Bourne シェル、および Korn シェルのデフォルトシステムプロンプトとスーパーユーザープロンプトを示しています。

表 **P–3** シェルプロンプト

シェル	プロンプト
C シェルプロンプト	`machine_name%`
C シェルのスーパーユーザープロンプト	`machine_name#`
Bourne シェルおよび Korn シェルのプロンプト	`$`
Bourne シェルおよび Korn シェルのスーパーユーザープロンプト	`#`

記号

次の表に、このマニュアルで使用する記号の表記規則をまとめています。

表 **P–4** 記号の表記規則

記号	説明	例	意味
[ ]	オプションのコマンドオプションに使用します。	`ls [-l]`	`-l` オプションは必須ではありません。
{ | }	必須コマンドオプションの選択項目に使用します。	`-d {y|n}`	`-d` オプションには `y` 引数か `n` 引数のいずれかを使用する必要があります。
-	同時に押す複数のキー入力を結合します。	Ctrl-A	Ctrl キーを押しながら A キーを押します。
+	連続的に押す複数のキー入力を結合します。	Ctrl+A+N	Ctrl キーを押し、離してから、後の 2 つのキーを押します。
>	グラフィカルユーザーインタフェースのメニュー項目の選択肢を表します。	File > New > Templates	「ファイル」メニューから「新規」を選択します。「新規」サブメニューから「テンプレート」を選択します。

デフォルトのパスとファイル名

次の表に、このマニュアルで使用するデフォルトのパスとファイル名を記載しています。

表 **P–5** デフォルトのパスとファイル名

内容	説明
msg_svr_base	Messaging Server の基本インストールディレクトリを表します。*msg_svr_base* インストールのデフォルト値は次のように表されます。 Solaris ™ システム: `/opt/SUNWmsgsr` Linux システム: `/opt/sun/messaging`
da_base	Delegated Administrator の基本インストールディレクトリを表します。 *da_base* インストールのデフォルト値は、次のとおりです。 Solaris ™ システム: `/opt/SUNWcomm` Linux システム: `/opt/sun/comms/commcli`

ユーザーからのご意見

Sun は当社のマニュアルの改善のために、ユーザーからのご意見ご提案を受け付けています。

ご意見をいただくには、`http://docs.sun.com` のページから 「コメントの送信」をクリックしてください。オンラインフォームに文書のタイトルとパーツ番号を入力してください。パーツ番号はこのマニュアルの表紙または最初に示されている 7 桁か 9 桁の数字です。たとえば、このマニュアルのタイトルは『Sun Java System Communications Services 2005Q4 Delegated Administrator 管理ガイド』、パーツ番号は 819-4103 です。

第 1 章

Delegated Administrator の概要

Communications Services Delegated Administrator のユーティリティーとコンソールを使用すると、Messaging Server や Calendar Server などの Communications Services アプリケーションで使用される LDAP ディレクトリでユーザー、グループ、ドメイン、リソースをプロビジョニングできます。

この章では次の項目について説明します。

はじめに

Delegated Administrator を使用した場合、LDAP ディレクトリの特定の組織を管理する権限を持つ下位の管理者に、プロビジョニング作業を分散することができます。ユーザー管理を委任できることにより、次の利点がもたらされます。

- 時間を要する大規模なディレクトリのプロビジョニングに対する責任を、多くの管理者に分散します。数十名、または数百名の管理者が、莫大な数のユーザーから構成される組織を 1 つのディレクトリ内で管理できます。
- はっきりと区別できる一意の単位として管理およびプロビジョニングが可能な組織を、ディレクトリ構造で作成できます。これらの組織には、顧客の業務、企業の部署、その他のグループに属するユーザーが含まれます。

Delegated Administrator では、2 種類のインタフェースを使用してディレクトリのユーザーおよび組織をプロビジョニングします。

- 24 ページの「Delegated Administrator コンソール」

以降の項で、これらのインタフェースについてまとめています。

Delegated Administrator ユーティリティー

Delegated Administrator ユーティリティーは、Messaging Server と Calendar Server の組織、ユーザー、グループ、およびカレンダリソースをプロビジョニングするためのコマンド行ツールセットです。

注 – Delegated Administrator ユーティリティーには、以前リリースされた Communications Services 製品 (Messaging Server 6 2005Q1 と Calendar Server 6 2005Q1) で使用できたコマンド行機能があります。Delegated Administrator ユーティリティーには、このマニュアルで説明するサービスプロバイダのロールと組織を作成するためのコマンドはありません。ロールと組織を新規に作成し、管理する場合、Delegated Administrator コンソールを使用する必要があります。

このユーティリティーは `commadmin` コマンドを使用して起動します。

`commadmin` ユーティリティーで使用できる構文とオプションの詳細については、第 5 章を参照してください。

Delegated Administrator コンソール

Delegated Administrator コンソールは、Messaging Server と Calendar Server の組織、ユーザー、グループ、およびカレンダリソースをプロビジョニングするためのグラフィカルユーザーインタフェース (GUI) です。

コンソールの使用方法については、Delegated Administrator コンソールのオンラインヘルプを参照してください。

Delegated Administrator と LDAP ディレクトリ

Delegated Administrator では、LDAP ディレクトリを変更してユーザーをプロビジョニングできます。ディレクトリを直接変更する必要はありません。ただし、ディレクトリのユーザーエントリと高位のノードに追加される Delegated Administrator の属性を理解しておくと役に立つ場合があります。

Delegated Administrator をサポートする LDAP スキーマのオブジェクトクラスと属性については、『*Sun Java System Communications Services Schema Reference*』の第 5 章「Communications Services Delegated Administrator Classes and Attributes (Schema 2)」を参照してください。

ユーザーのプロビジョニングのシナリオ

ビジネス上のニーズに応じて、1 人の管理者で管理される簡単なディレクトリ構造、またはプロビジョニング作業および管理作業が下位の管理者に委任される多層ディレクトリ階層を作成できます。

この項では複雑さが増す 3 つのシナリオをまとめています。次に、これらのシナリオの要件をサポートするために Delegated Administrator が提供する管理者のロールとディレクトリ構造を説明します。

単層階層

このシナリオでは、企業または組織が数百または数千の従業員またはユーザーをサポートしている場合を想定しています。すべてのユーザーは 1 つの組織にグループ化されます。単一の管理者のロールでグループ全体が表示され、管理されます。管理作業の委任は起こりません。

図 1–1 に単一組織、単層階層での管理者のロールの例を示します。

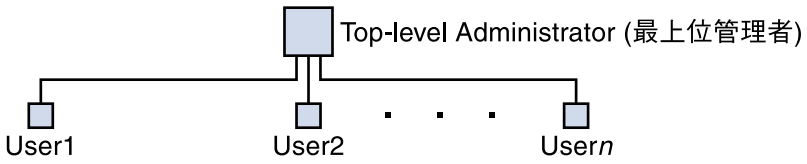

図 **1–1** 単層階層の管理者のロール

この単層階層では、管理者は最上位管理者 (Top-Level Administrator) (TLA) と呼ばれます。

図 1–1 に示す例では、TLA はユーザー (User1、User2 ～ Usern) を直接管理し、プロビジョニングします。

ディレクトリの組織が 1 つの場合、必要な管理者はTLA だけです。

詳細は、次の項を参照してください。

- 28 ページの「単層階層をサポートするディレクトリ構造」
- 29 ページの「最上位管理者のロール」

2 層階層

このシナリオでは、インターネットサービスプロバイダ (ISP) などの大企業がビジネス向けにサービスを提供しています。各ビジネスには数千、数万のユーザーを抱える固有のドメインがあります。

すべてのドメインの管理およびプロビジョニングを単一の最上位管理者 (TLA) に依存するのではなく、このシナリオでは下位の管理者への作業の委任をサポートしています。

2 層階層では、ディレクトリに複数の組織が含まれています。各ホストドメインに個別の組織が作成されます。

各組織に組織管理者 (Organization Administrator) (OA) が割り当てられます。OA はその組織のユーザーに対する責任を負います。OA はその OA の組織の外部のディレクトリ情報を表示したり、変更したりすることはできません。

図 1–2 に 2 層階層での管理者のロールの例を示します。

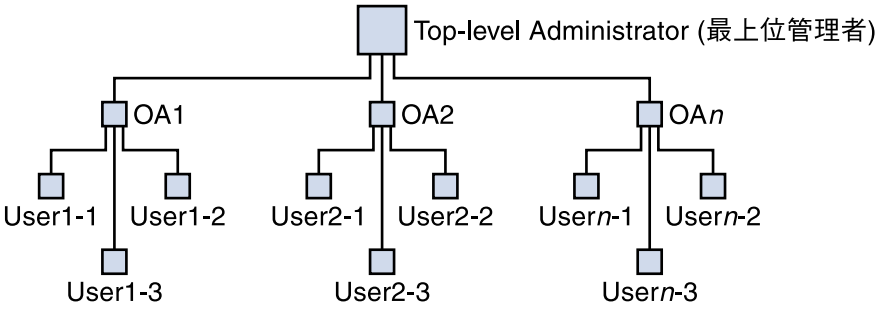

図 **1–2** 2 層階層の管理者のロール

図 1–2 に示す例では、TLA は OA1、OA2 ～ OAn を作成し、管理します。各 OA は 1 つの組織のユーザーを管理します。

ディレクトリに複数の組織が必要になる場合、TLA と OA を作成し組織とそのユーザーを管理します。

詳細は、次の項を参照してください。

- 29 ページの「2 層階層をサポートするディレクトリ構造」
- 29 ページの「最上位管理者のロール」
- 30 ページの「組織管理者のロール」

3 層階層

このシナリオでは、ISP などの企業がそれぞれ独自の組織を必要とする数百または数千の小規模ビジネスにサービスを提供しています。

ISP はメールサービスを必要とする数百万のエンドユーザーをサポートする場合があります。さらに、ISP はエンドユーザーのビジネスを管理するサードパーティ再販業者と連携して作業する場合があります。

毎日、数十の新しい組織をディレクトリに追加する必要も生じます。

2 層階層では、TLA がこのような組織の新規作成を担当します。

3 層階層では、管理タスクは第 2 レベルの管理者に委任されます。この第 2 レベルの委任により、大規模な LDAP ディレクトリでサポートされる大規模な顧客ベースの管理が軽減される場合があります。

この階層をサポートするために、Delegated Administrator は新しいロールであるサービスプロバイダ管理者 (SPA) を導入します。

SPA の権限範囲は、最上位管理者 (TLA) から組織管理者 (OA) までの間です。

図 1–3 に 3 層階層での管理者のロールの例を示します。

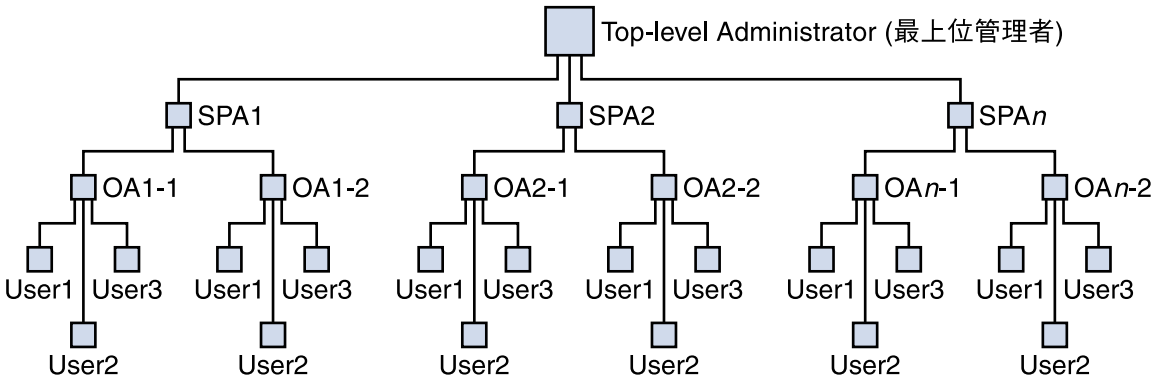

図 **1–3** 3 層階層の管理者のロール

3 層階層では、TLA は管理権限をサービスプロバイダ管理者 (SPA) に委任します。SPA は新規顧客のために下位組織を作成し、その下位組織のユーザーを管理する組織管理者 (OA) を割り当てられます。

サブグループまたは組織に分割される複数の組織が必要になる場合、TLA、SPA、OA の各ロールを実装する 3 層階層を使用できます。

SPA のロールについては、付録 A を参照してください。

管理者のロールとディレクトリ階層

この項では単層階層および 2 層階層を実装するディレクトリ情報ツリーの例を示します。次に最上位管理者と組織管理者で実行できるタスクについて説明します。

単層階層をサポートするディレクトリ構造

設定プログラム `config-commda` を実行して Delegated Administrator を設定するときに、最上位管理者 (TLA) とデフォルト組織を作成します。

単層階層: ルートサフィックス下のデフォルト組織

デフォルトでは、設定プログラムによりデフォルト組織はルートサフィックスの下に置かれます。

ディレクトリ情報ツリーは、図 1–4 のような形式になります。

図 1–4 に単層階層で編成されたディレクトリ情報ツリーの例を示します (デフォルト設定)。

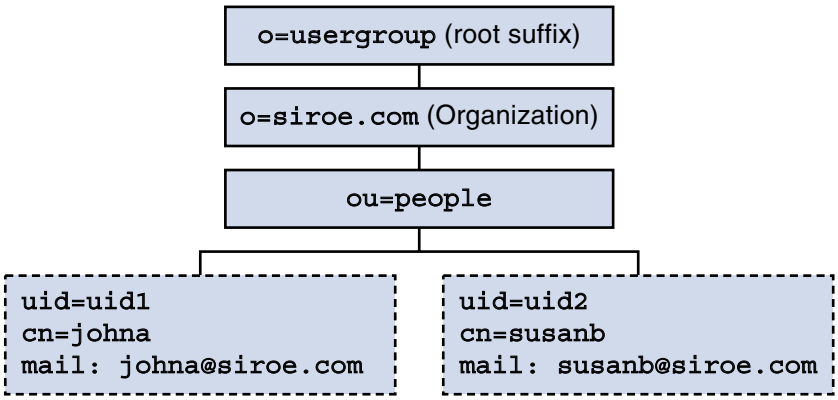

図 **1–4** 単層階層: ディレクトリ情報ツリー (デフォルト) の例

単層階層: ルートサフィックスのデフォルト組織

設定プログラム `config-commda` を実行する場合、ルートサフィックスの下ではなく、ルートサフィックスと同じレベルでデフォルト組織を作成できます。設定の詳細については、第 3 章の 69 ページの「Delegated Administrator サーバーの設定」を参照してください。

この場合、ディレクトリ情報ツリーは図 1–5 に示すような構成になります。

ただし、ルートサフィックスのレベルでデフォルト組織を作成する場合、この設定の LDAP ディレクトリは複数のホストドメインをサポートできません。複数のホストドメインをサポートする場合、デフォルト組織をルートサフィックスの下に置く必要があります。

図 1–5 に、デフォルト組織がルートサフィックスのレベルに作成された単層階層の例を示します。

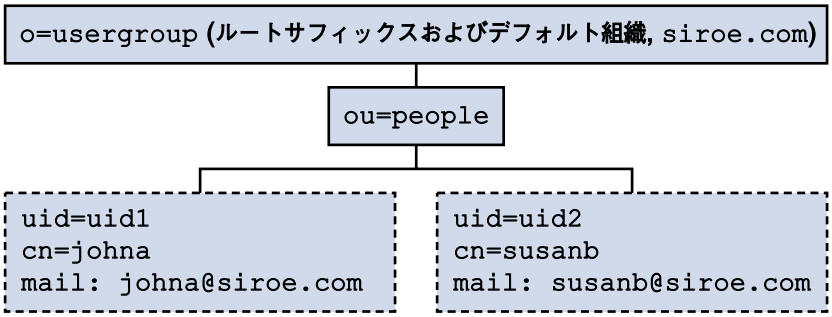

図 **1–5** 単層階層: ルートサフィックスのデフォルト組織

2 層階層をサポートするディレクトリ構造

`config-commda` プログラムでの Delegated Administrator の設定後、TLA は図 1–6 で示すような新しい組織を追加で作成できます。

図 1–6 に 2 層階層で編成されたディレクトリ情報ツリーの例を示します。

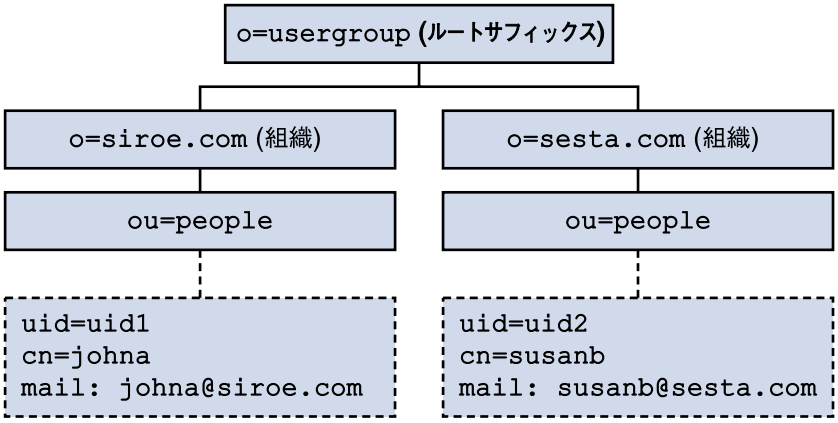

図 **1–6** 2 層階層: ディレクトリ情報ツリーの例

最上位管理者のロール

TLA には次の作業を実行する権限があります。

- 組織を作成、削除、変更する。

図 1–6 に示す例では、TLA は siroe.com や sesta.com の変更と削除、および新しい組織の作成を行うことができます。

この例では、2 つの組織も一意のホストドメインであることに注意してください。

- ユーザーを作成、削除、変更する。
- グループを作成、削除、変更する。
- カレンダリソースを作成、削除、変更する。
- ユーザーへの OA のロールの割り当て。たとえば、TLA は組織 siroe.com のユーザー johna に OA のロールを割り当てることができます。

  TLA はユーザーから OA のロールを削除することもできます。
- その他のユーザーに TLA のロールを割り当てる。TLA はユーザーから TLA のロールを削除することもできます。
- 組織にサービスパッケージを割り当てる。

  サービスパッケージの詳細については、この章の後半で説明する 32 ページの「サービスパッケージ」を参照してください。

  TLA は指定されたタイプのサービスパッケージを組織に割り当て、各パッケージについて、その組織で使用できる回数の上限を決定できます。

  たとえば、TLA は次のサービスパッケージを割り当てられます。

  - 組織 siroe.com

    1,000 gold パッケージ

    500 platinum パッケージ
  - 組織 sesta.com

    2,000 silver パッケージ

    1,500 gold パッケージ

    100 platinum パッケージ

    TLA が上記のタスクを実行するには、Delegated Administrator コンソールを使用するか、Delegated Administrator ユーティリティー (commadmin) のコマンドを実行します。

    commadmin コマンドの詳細については第 5 章の表 5–1 を参照してください。

組織管理者のロール

OA には、OA の組織内で次の作業を実行する権限があります。

- ユーザーを作成、削除、変更する。

  図 1–6 に示す例では、ユーザー johna に組織 siroe.com の OA のロールが割り当てられている場合、johna は siroe.com のユーザーを管理できます。
- グループを作成、削除、変更する。
- カレンダリソースを作成、削除、変更する。

- その他のユーザーに OA のロールを割り当てる。
- ユーザーに対してサービスパッケージを割り当て、削除する。

OA は、OA の組織外のユーザー、グループ、またはリソースに対しては、これらの作業を実行できません。

たとえば、図 1–6 に示すように `johna` が `siroe.com` の OA である場合、 `johna` は `sesta.com` のユーザー、グループ、またはリソースを管理できません。

OA が上記のタスクを実行するには、Delegated Administrator コンソールを使用するか、Delegated Administrator ユーティリティー (`commadmin`) コマンドを実行します。

OA が使用できる `commadmin` コマンドの詳細については第 5 章の表 5–1 を参照してください。

以前の iPlanet Delegated Administrator ユーザーについて

Communications Services Delegated Administrator は、LDAP Schema 2 ディレクトリでのユーザーのプロビジョニング向けに設計されています。

LDAP Schema 1 ディレクトリを持つ以前のバージョンの Messaging Server のユーザーは、非推奨ツールである iPlanet Delegated Administrator を使用している場合があります。現在も Shema 1 ディレクトリが存在する場合、iPlanet Delegated Administrator を使用してユーザーをプロビジョニングすることをお勧めします。

iPlanet Delegated Administrator で使用する管理者のロールについての用語は、Communications Service Delegated Administrator で現在使用されているものとは多少異なります。

表 1–1 に、各バージョンの Delegated Administrator の管理者のロールとその定義を示します。

表 **1–1** iPlanet Delegated Administrator と Communications Services Delegated Administrator の管理者のロール

iPlanet Delegated Administrator	**Communications Services Delegated Administrator** ユーティリティー	**Communications Services Delegated Administrator** コンソール	定義
サイト管理者	最上位管理者 (TLA)	最上位管理者 (TLA)	組織とユーザーを含む、Delegated Administrator でサポートされるディレクトリ全体を管理します*。
(なし)	(このリリースではなし)	サービスプロバイダ管理者 (SPA)	プロバイダ組織。プロバイダ組織内の共有される完全なビジネス組織およびそれらのビジネス組織のユーザーを管理します。
ドメイン管理者	組織管理者 (OA)	組織管理者 (OA)	1 つの組織およびその組織のユーザーを管理します。
* Delegated Administrator の今回のリリースでは、TLA はプロバイダ組織またはプロバイダ組織の下のビジネス組織を作成できません。			

サービスパッケージ

サービスパッケージは LDAP ディレクトリのサービスクラスメカニズムによって実装されています。このメカニズムにより、Delegated Adminsitrator を設定したときにディレクトリにインストールされる定義済みの属性に値を設定できます。サービスパッケージは、ユーザーエントリまたはグループエントリにサービスの特徴を追加します。

Delegated Administrator には、サンプルサービスクラステンプレートが用意されています。

また、独自のサービスパッケージを作成することもできます。

Delegated Administrator コンソールでは、サンプルパッケージや独自のパッケージをユーザーまたはグループに割り当てることができます。

サービスパッケージのタイプ

サービスパッケージには次のコンポーネントが含まれます。

- Access Manager サービス
- サービスバンドル (メールサービスまたはカレンダサービス、あるいはその両方)
- LDAP オブジェクト (ユーザーまたはグループ)

Delegated Administrator は Access Manager サービスに各サービスの定義を自動的に提供します。サービスパッケージをユーザーまたはグループに割り当てると、Delegated Administrator はサービス定義から Access Manager のオブジェクトクラスと属性を取得し、それらを LDAP エントリに追加します。

サービスパッケージの Access Manager の部分は、いずれも変更したり削除したりしないでください。

サービスパッケージの作成時には、そのサービスパッケージのサービスバンドルと LDAP オブジェクトを設定できます。

サービスバンドル

Delegated Administrator は 2 つのタイプのサービスを提供します。メールサービスとカレンダサービスです。

サービスパッケージは 1 つ以上のサービスを、そのサービスに関連付けられた属性セットとともにバンドルします。したがって、個々のサービスパッケージには次のサービスの組合わせを含むことができます。

- メールサービスのみ
- カレンダサービスのみ
- メールサービスとカレンダサービス

注 – サービスクラス定義に LDAP 属性があるのはメールサービスのみです。カレンダサービスに関連付けられている属性はありません。

特定の LDAP オブジェクトに対して定義されたパッケージ

サービスパッケージは、ユーザーまたはグループに対して定義されます。ユーザーとグループに同じサービスパッケージを割り当てることはできません。

Delegated Administrator は、次のサービスバンドルと LDAP オブジェクトを持つサービスパッケージを提供しています。

- ユーザーメールサービス
- ユーザーカレンダサービス

- ユーザーメールとカレンダサービス
- グループメールサービス

注 – グループには、メールサービスだけを割り当てることができます。このリリースの Delegated Administrator では、グループはカレンダサービスを持つことができません。

グループについて

Delegated Administrator では、グループとはユーザーのリストで構成される LDAP ディレクトリのエントリです。グループのメンバーであるユーザーに、グループの特徴は受け渡されません。たとえば、サービスパッケージをグループに割り当てると、グループのメンバーであるユーザーに、サービスパッケージの属性は継承されません。

メールサービスパッケージがグループに割り当てられると、グループは Messaging Server が利用するメーリングリストになります。

Delegated Administrator が提供するサービスパッケージ

Delegated Administrator の設定時には、事前定義済みのサンプルサービスクラステンプレートのセットをインストールすることを選択できます。Delegated Administrator コンソールには、これらのテンプレートが表示されます。

(設定プログラムを実行するときに、「サービスパッケージと組織のサンプル」パネルで「サンプルサービスパッケージを読み込む」を選択してください。)設定プログラムによって、`cos.sample.ldif` ファイルが LDAP ディレクトリに追加されます。

サンプルテンプレートを使用すると、サービスとメール属性をユーザーとグループに提供できます。テンプレートとその属性値の一覧については、39 ページの「サンプルサービスクラステンプレート」を参照してください。

サンプルサービスクラステンプレートを使用しない場合は、スケルトン ldif ファイルを修正して、LDAP ディレクトリとコンソール表示からテンプレートを削除できます。

図 1–7 に、ユーザーサービスパッケージのテンプレートを示します。

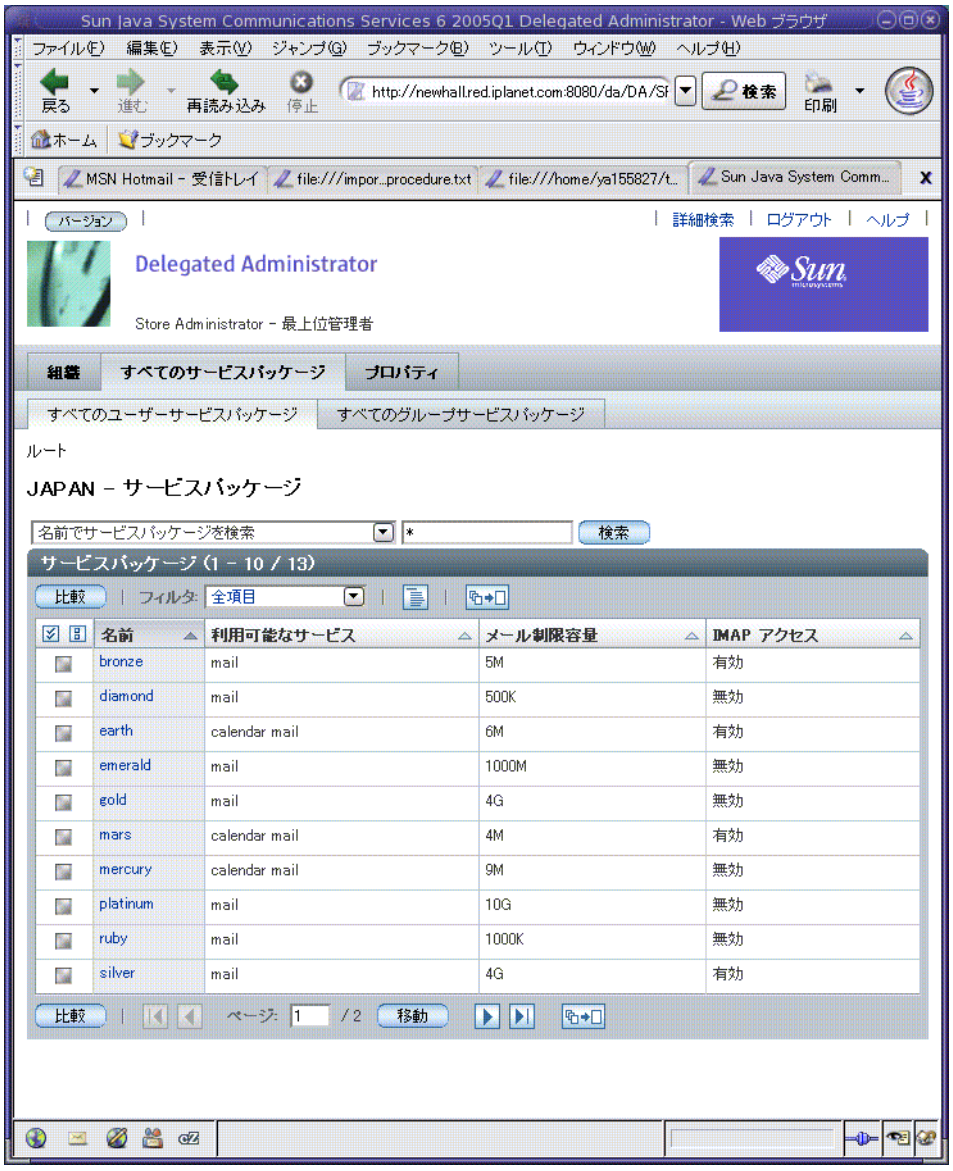

図 **1–7** サンプルテンプレートを表示する「すべてのユーザーサービスパッケージ」ページ

図 1–8 に、グループサービスパッケージのテンプレートを示します。

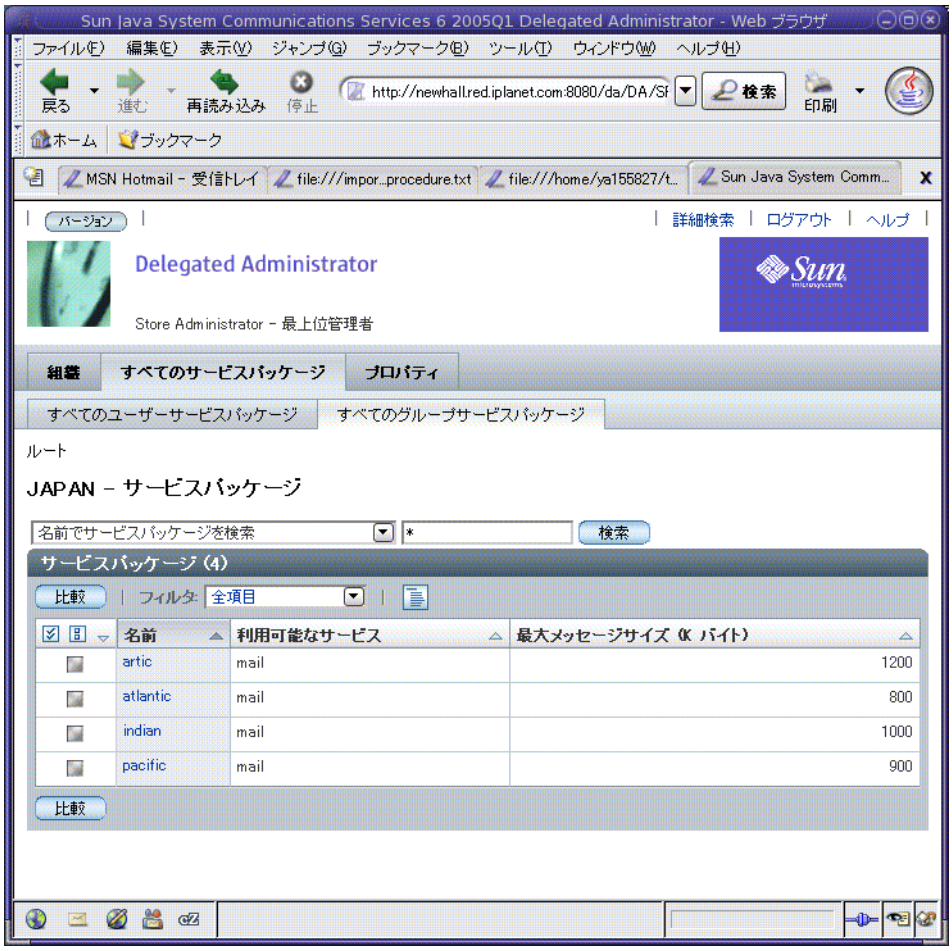

図 1–8 サンプルテンプレートを表示する「すべてのグループサービスパッケージ」ページ

サービスパッケージのタスク

Delegated Administrator コンソールで、次のサービスパッケージのタスクを行います。

- 組織へのサービスパッケージの割り当て。組織に一部の (またはすべての) パッケージを割り当てることで、組織のユーザーまたはグループがパッケージを使用できるようになります。

  各パッケージについて、指定された数のパッケージを割り当てます。

  たとえば、ABC という組織に 5,000 の gold サービスパッケージ、10,000 の venus サービスパッケージ、および 500 の atlantic サービスパッケージを割り当てる場合などです。

- ユーザーへのサービスパッケージの割り当て。
- グループへのサービスパッケージの割り当て。

サービスパッケージの割り当てに関するガイドライン

- 組織に割り当てられたサービスパッケージによって構成されるプールを使用して、サービスパッケージを組織内のユーザーまたはグループに割り当てることができます。
- 1 ユーザーまたは 1 グループに複数のサービスパッケージを割り当てられます。
- 1 ユーザーまたは 1 グループに 1 つのサービスパッケージを割り当てると、そのサービスパッケージのすべての属性および値がユーザーまたはグループに自動的に割り当てられます。
- カレンダサービスだけをユーザーに割り当てるには、standardUserCalendar サービスパッケージを使用します。カレンダサービスには、関連付けられた属性がありません。

  standardUserCalendar サービスパッケージを割り当てると、`commadmin user create` コマンドまたは `commadmin user modify` コマンドで `-s cal` オプションを使用するのと同じ結果が得られます。

サービスパッケージの割り当て方法については、Delegated Administrator コンソールのオンラインヘルプを参照してください。

独自のサービスパッケージの作成

この章で説明するサービスクラステンプレートは、例示を目的としたものです。実際のインストールでは、ユーザーやグループに対して適切な属性値を使用して独自のサービスパッケージを作成することが多くあります。

独自のサービスパッケージを作成するには、`da.cos.skeleton.ldif` ファイルに保存されているサービスクラステンプレートを利用できます。このファイルは、サービスパッケージのテンプレートとして使用するために作成されたものです。Delegated Administrator を設定するときには、このファイルは LDAP ディレクトリにインストールされません。

`da.cos.skeleton.ldif` ファイルをコピーして編集し、`ldapmodify` などの LDAP ディレクトリツールを使用して、カスタマイズしたサービスクラステンプレートをディレクトリにインストールできます。

Delegated Administrator コンソールには、カスタマイズしたテンプレートがサンプルテンプレートとともに表示されます。コンソールではサービスクラステンプレートはサービスパッケージと呼ばれます。サービスパッケージをユーザーまたはグループのいずれかに割り当てることができる場合、Delegated Administrator は Access Manager サービスを含む完全なサービスパッケージをユーザーまたはグループの LDAP エントリに配置します。

da.cos.skeleton.ldif ファイルを使用して独自のサービスパッケージを設定する方法については、第 3 章の 77 ページの「サービスパッケージの作成」を参照してください。

拡張サービスパッケージの表示に関する制限

Delegated Administrator サービスパッケージの定義は、定義エントリに属性を追加することによって拡張できます。

ただし、Delegated Administrator の今回のリリースでは、Delegated Administrator を設定するときコンソールに表示できるのは定義済みの属性だけです。Delegated Administrator コンソールに、サービスパッケージ定義に追加した属性は表示されません。

このリリースでは、Delegated Administrator が提供するサービスクラス定義から定義済み属性を削除しないでください。

LDAP エントリに割り当てられるサンプルサービスパッケージ

Delegated Administrator を使用してユーザーまたはグループにサービスパッケージを割り当てる場合、LDAP ディレクトリのユーザーエントリまたはグループエントリに 1 つの属性 (inetCOS) が追加されます。inetCOS 属性の値により、サービスとそのサービスに関連付けられたすべての属性を含むサービスパッケージ全体がユーザーまたはグループに割り当てられます (inetCOS は多値属性)。

たとえば、platinum パッケージをユーザーに割り当てる場合を想定してください。次の属性がユーザーエントリに追加されます。

```
inetCOS: platinum
```

platinum パッケージはユーザーにメールサービスを提供します。また、このパッケージにはメール属性について次の値が含まれます。この場合、platinum パッケージを割り当てることで、ユーザーエントリにこれらの属性が追加されるという効果があります。

```
mailMsgMaxBlocks: 800
mailQuota: 10000000
mailMsgQuota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
```

Access Manager サービスの定義によって、メールサービスまたはカレンダサービス、あるいはその両方に必須のオブジェクトクラスと属性が提供されます。このサービスパッケージを割り当てると、Delegated Administrator はこれらのオブジェクトクラスと属性をユーザーエントリまたはグループエントリに追加します。

サンプルサービスクラステンプレート

この項では、サンプルサービスクラステンプレートと、テンプレートが提供するメール属性値を示します。

これらのテンプレートは cos.sample.ldif ファイル内にあります。

メールサービス属性

メールサービスには、メールユーザーに対して定義される LDAP 属性が含まれます。表 1–2 に、これらの属性の定義を示します。

表 **1–2** サービスパッケージで使用されるメールサービス属性

属性	定義
mailMsgMaxBlocks	ユーザーまたはグループに送信できる最大メッセージの MTA ブロックの単位サイズ。
mailAllowedServiceAccess	指定されたサービスへのアクセスが可能なクライアントを指定するフィルタ。例 : +imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
mailMsgQuota	ユーザーに許可された最大メッセージ数 (すべてのユーザーフォルダを含む)。
mailQuota	ユーザーのメールボックスに指定できるディスク容量 (バイト)。

これらの属性の詳細については、『*Sun Java System Communications Services Schema Reference*』の第 3 章「Messaging Server and Calendar Server Attributes」を参照してください。

ユーザーメールサンプルテンプレート

Platinum

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Gold

```
mailMsgMaxBlocks: 700
mailquota: 8000000
```

```
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Silver

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Bronze

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Ruby

```
mailMsgMaxBlocks: 600
mailquota: 1048576
mailmsgquota: 2000
mailAllowedServiceAccess: +pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Emerald

```
mailMsgMaxBlocks: 600
mailquota: 2097152
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

Diamond

```
mailMsgMaxBlocks: 5000
mailquota: 3145728
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
```

Topaz

```
mailMsgMaxBlocks: 3000
mailquota: 4194304
mailmsgquota: 2000
mailAllowedServiceAccess: +imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
```

ユーザーカレンダサンプルテンプレート

なし *(standardUserCalendar)*

カレンダサービスを提供し、属性値を含む定義済みサービスクラステンプレートはありません。カレンダサービスは、属性値の関連付けなしで提供されます。

サンプルテンプレートが存在しないので、Delegated Administrator はテンプレートを使用せずにユーザーカレンダサービスクラス定義から直接、デフォルトのサービスパッケージを生成します。その名前は、サービスクラス定義の名前と同じになります。つまり、standardUserCalendar です。

このサービスパッケージは、カレンダサービスのみを提供します。

ユーザーメールサンプルテンプレートとユーザーカレンダサンプルテンプレート

次のサンプルテンプレートはメールサービスとカレンダサービスの両方に適用されます。

Mercury

```
mailMsgMaxBlocks: 800
mailquota: 10000000
mailmsgquota: 6000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Venus

```
mailMsgMaxBlocks: 700
mailquota: 8000000
mailmsgquota: 3000
mailAllowedServiceAccess: +imaps:ALL$+pops:ALL$+smtps:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Earth

```
mailMsgMaxBlocks: 300
mailquota: 6291456
mailmsgquota: 2000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

Mars

```
mailMsgMaxBlocks: 700
mailquota: 5242288
mailmsgquota: 3000
mailAllowedServiceAccess: +pop:ALL$+imap:ALL$+smtp:ALL$+http:ALL
daServiceType: mail user
daServiceType: calendar user
```

グループメールサンプルテンプレート

Atlantic

```
mailMsgMaxBlocks: 800
daServiceType: mail group
```

Pacific

```
mailMsgMaxBlocks: 900
daServiceType: mail group
```

Indian

```
mailMsgMaxBlocks: 1000
daServiceType: mail group
```

Arctic

```
mailMsgMaxBlocks: 1200
daServiceType: mail group
```

サービスクラスの定義

このリリースの Delegated Administrator では、次の各種サービスパッケージに対するサービスクラスの定義が提供されています。

- ユーザーメールサービス
- ユーザーカレンダサービス
- ユーザーメールとカレンダサービス
- グループメールサービス

Delegated Administrator の設定時に、サービスクラスの定義がディレクトリにインストールされます。

各定義では、daServiceType 属性の次の構文によってサービスパッケージのタイプが決まります。

```
daServiceType: <service type> <target>
```

service type はメールサービスまたはカレンダサービス、あるいはその両方、*target* はユーザーまたはグループを示します。

ユーザーのメールサービス

ユーザーメールサービスは standardUserMail というサービスクラスの定義で定義されます。

```
#
#  Definition for user mail service bundle
#
dn: cn=standardUserMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: mail user
```

```
注: Delegated Administrator の設定プログラムによって
standardUserMail 定義をディレクトリにインストールすると、
上記の変数 <ugldapbasedn> はルートサフィックス
(o=usergroup など) に置き換えられます。
```

daServiceType 属性によって、これはユーザーのメールサービスとして定義されます。

ユーザーのカレンダサービス

ユーザーカレンダサービスは standardUserCalendar というサービスクラスの定義で定義されます。

```
#
#  Definition for user calendar service bundle
#
dn: cn=standardUserCalendar,<ugldapbasedn>
changetype: add
objectclass: top
```

```
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
daServiceType: calendar user


注: Delegated Administrator の設定プログラムによって
standardUserCalendar 定義をディレクトリにインストールすると、
上記の変数 <ugldapbasedn> はルートサフィックス
(o=usergroup など) に置き換えられます。
```

daServiceType 属性によって、これはユーザーのカレンダサービスとして定義されます。

注 – カレンダサービスの定義には、icsPreferredHost などのカレンダ属性も含まれることに注意してください。

ただし Delegated Administrator では、これらの属性値を指定するサービスパッケージテンプレートは用意されていません。Delegated Administrator コンソールは、カレンダサービスのみを持つサービスパッケージを 1 つだけ提供します。standardUserCalendar サービスパッケージです。このパッケージには、カレンダ属性が含まれません。

ユーザーのメールとカレンダサービス

ユーザーメールとカレンダサービスは standardUserMailCalendar というサービスクラスの定義で定義されます。

```
#
#  Definition for user mail and user calendar service bundle
#
dn: cn=standardUserMailCalendar,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: icsPreferredHost
cosAttribute: icsDWPHost
cosAttribute: icsFirstDay
cosAttribute: icsQuota
```

```
cosAttribute: mailAllowedServiceAccess
cosAttribute: mailMsgMaxBlocks
cosAttribute: mailquota
cosAttribute: mailmsgquota
daServiceType: calendar user
daServiceType: mail user
```

注: Delegated Administrator の設定プログラムによって standardUserMailCalendar 定義をディレクトリにインストールすると、上記の 変数 <ugldapbasedn> はルートサフィックス (o=usergroup など) に置き換えられます。

2 つの daServiceType 属性エントリによって、これはユーザーのカレンダサービスとメールサービスとして定義されます。

グループのメールサービス

グループメールサービスは standardGroupMail というサービスクラスの定義で定義されます。

```
#
#  Definition for group mail service bundle
#
dn: cn=standardGroupMail,<ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleObject
objectclass: cosSuperDefinition
objectclass: cosClassicDefinition
cosTemplateDn: o=cosTemplates,<ugldapbasedn>
cosSpecifier: inetCos
cosAttribute: mailMsgMaxBlocks
daServiceType: mail group
```

注: Delegated Administrator の設定プログラムによって standardGroupMail 定義をディレクトリにインストールすると、上記の変数 <ugldapbasedn> はルートサフィックス (o=usergroup など) に置き換えられます。

daServiceType 属性によって、これはグループのメールサービスとして定義されます。

サービスクラス定義とパッケージの場所

LDAP ディレクトリ情報ツリー (DIT) では、サービスクラス定義はルートサフィックス直下のノードに格納されます。サービスパッケージは DIT のトップに置かれるため、ディレクトリの全ユーザーエントリに割り当てられます。

図 1–9 に、サービス定義とパッケージの DIT での場所を示します。

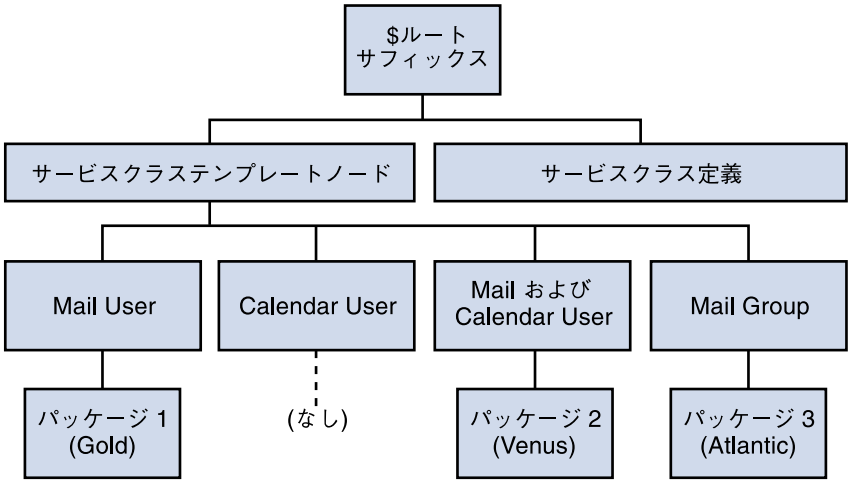

図 **1–9** サービスクラス定義とパッケージのディレクトリツリー内の場所

各種サービスクラステンプレートは、それぞれ独自のノード下に格納されます。したがって、ユーザーにメールサービスを提供するテンプレートは Mail User ノードの下に格納されます。この構造によって、Delegated Administrator はユーザーまたはグループにサービスパッケージを割り当てるときに正しいサービスクラスの定義 (`standardUserMail` など) を使用できます。

Delegated Administrator は標準的なサービスクラス定義を使用します。

サービスクラスの仕組みの詳細については、『*Sun Java System Directory Server* 管理ガイド』を参照してください。特に、第 5 章「ID とロールの管理」の「サービスクラス (CoS) の定義」を参照してください。

『*Sun Java System Directory Server* 管理ガイド』では、サービスパッケージで定義されユーザーに割り当てられた属性がすでにその個々のユーザーエントリ内にある場合に優先されるサービス属性の値の判断など、関連項目についても説明しています。

第 2 章

インストールおよび設定の計画

Solaris システムで Sun Java System Communications Services Delegated Administrator をインストールする場合、Sun Java Enterprise System インストーラを使用する必要があります。このインストーラにより、ほかの Sun コンポーネント製品もインストールされます。

Delegated Administrator をインストールし設定するには、次の手順に従います。

1. 47 ページの「Delegated Administrator 設定情報の収集」
2. 51 ページの「Java Enterprise System インストーラの実行」
3. 53 ページの「Directory Server セットアップスクリプトの実行」
4. 53 ページの「Delegated Administrator の設定」
5. 54 ページの「Messaging Server と Calendar Server の設定」

   Delegated Administrator に関する最新の情報については、『Sun Java System Communications Services リリースノート』を参照してください。

Delegated Administrator 設定情報の収集

Delegated Administrator コンポーネント

Delegated Administrator は、次のコンポーネントから構成されます。

- **Delegated Administrator Utility (client)** — `commadmin` で呼び出されるコマンド行インタフェース。

  必須。Delegated Administrator をインストールするすべてのマシンに、このユーティリティーを設定する必要があります。

- **Delegated Administrator Server** — Delegated Administrator のユーティリティーとコンソールを実行するのに必要な Delegated Administrator サーバーコンポーネント。

  必須。少なくとも 1 台のマシンに Delegated Administrator サーバーを設定する必要があります。

- **Delegated Administrator** コンソール — Delegated Administrator グラフィカルユーザーインタフェース (GUI)。

  オプション。Delegated Administrator ユーティリティーのみを使用する場合、コンソールを設定する必要はありません。

Web コンテナ

また、Delegated Administrator のサーバーとコンソールは Web コンテナにも配備する必要があります。Delegated Administrator のコンソールとサーバーは次のプラットフォームに設定できます。

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

次のガイドラインに従います。

- Delegated Administrator サーバーを、Access Manager で使用される Web コンテナに配備する必要があります。
- Delegated Administrator のコンソールとサーバーは、2 つの異なる Web コンテナ、Web コンテナの 2 つの異なるインスタンス、または同じ Web コンテナに配備できます。

設定情報

Delegated Administrator を設定する前に、設定情報を集める必要があります。

表 2–1 に Delegated Administrator に必要な設定オプションを示します。

表 2–2 に Web Server に配備するための設定オプションを示します。

表 2–3 に Application Server 7.*x* に配備するための設定オプションを示します。

表 2–4 に Application Server 8.*x* に配備するための設定オプションを示します。

表 **2–1** Delegated Administrator 必要な設定オプション

オプション	説明
設定ディレクトリ	設定およびデータファイルを保存するディレクトリ。
Access Manager ホスト名	Access Manager がインストールされるホスト名。Delegated Administrator サーバーは同じサーバーにインストールします。
Access Manager ポート番号	Access Manager のポート番号。Web Server のポート番号と同じになります。
デフォルトドメイン	最上位管理者のデフォルトドメイン。`commadmin` コマンド行ユーティリティーを実行する場合に、ドメインが `-n` オプションにより明示的に指定されないときに使用されるドメインです。
デフォルト SSL ポート	Delegated Administrator クライアントで使用される SSL ポート。
Access Manager ベースディレクトリ	Access Manager がインストールされるディレクトリ。デフォルトディレクトリは `/opt/SUNWam` です。
LDAP URL	ユーザーおよびグループの Directory Server LDAP URL。
バインド	ユーザーおよびグループの Directory Server ディレクトリマネージャー。例「cn=Directory Manager」。
LDAP パスワード	ユーザーとグループのディレクトリマネージャーパスワード。
Access Manager 最上位管理者ユーザーの ID とパスワード	Access Manager 最上位管理者のユーザー ID とパスワード。
Access Manager 内部 LDAP 認証ユーザーのパスワード	Access Manager で作成されたユーザー。これは LDAP サービスのバインド DN ユーザーです。
組織名	デフォルト電子メールドメインに属するすべての電子メールユーザーとグループが配置される LDAP サブツリーに命名するために使用されます。
デフォルト組織のユーザー ID とパスワードに対する最上位管理者	デフォルト組織で作成される最上位管理者のユーザー ID とパスワード。
サンプル組織の優先メールホスト	Messaging Server がインストールされているマシンの名前。ディレクトリへのサンプル組織のインストールを決定した場合、優先メールホストを入力する必要があります。

表 **2–2** Web Server 設定オプション

オプション	説明
Web Server ルート (インスタンス) ディレクトリ	Web Server インスタンスが置かれるディレクトリ。Web Server インスタンスのファイルは、Web Server インストールディレクトリ内の `https-`*host* `.`*domain* ディレクトリに格納されます。

表 **2–2** Web Server 設定オプション　(続き)

オプション	説明
Web Server インスタンス識別子	Web Server インスタンスの完全修飾ドメイン名。これは `west.sesta.com` などの *host.domain* 名で指定できます。
仮想サーバー識別子	`https-west.sesta.com` などの `https-`*host.domain* 名で指定されます。
HTTP ポート番号	Web Server の HTTP ポート番号。

表 **2–3** Application Server 7.*x* 設定オプション

オプション	説明
Application Server インストールディレクトリ	Application Server 7.*x* がインストールされたディレクトリ。デフォルトでは、このディレクトリは `/opt/SUNWappserver7` になります。
Application Server ドメインディレクトリ	デフォルトでは、このディレクトリは `/var/opt/SUNWappserver7/domains/domain1` になります。
Application Server ドキュメントルートディレクトリ	デフォルトでは、このディレクトリは `/var/opt/SUNWappserver7/domains/domain1/server1/docroot` になります。
Application Server インスタンス名	インスタンス名。例 : `server1`
仮想サーバー識別子	Application Server の仮想サーバー識別子の名前。例 : `server1`
Application Server インスタンス HTTP ポート番号	Application Server インスタンスの HTTP ポート番号。
Administration Server ポート番号	Application Server 7. *x* の Administration Server インスタンスのポート番号。例 : `4848`
Administration Server 管理者のユーザー ID とパスワード。	Administration Server 管理者のユーザー ID とパスワード。ユーザー ID 例: `admin`
Administration Server インスタンスへの HTTP または HTTPS アクセス	Administration Server インスタンスへの HTTP アクセスをセキュリティー保護するかどうかを指定する必要があります。

表 **2–4** Application Server 8.*x* 設定オプション

オプション	説明
Application Server インストールディレクトリ	Application Server 8.*x* がインストールされたディレクトリ。デフォルトでは、このディレクトリは `/opt/SUNWappserver/appserver` になります。

表 2–4 Application Server 8.*x* 設定オプション　(続き)

オプション	説明
Application Server ドメインディレクトリ	デフォルトでは、このディレクトリは `/var/opt/SUNWappserver/domains/domain1` になります。
Application Server ドキュメントルートディレクトリ	デフォルトでは、このディレクトリは `/var/opt/SUNWappserver/domains/domain1/docroot` になります。
Application Server ターゲット名	インスタンス名。例 : `server`
仮想サーバー識別子	Application Server の仮想サーバー識別子の名前。例 : `server`
Application Server ターゲット HTTP ポート番号	Application Server ターゲットの HTTP ポート番号。
Administration Server ポート番号	Application Server 8. *x* の Administration Server インスタンスのポート番号。例 : `4849`
Administration Server 管理者のユーザー ID とパスワード。	Administration Server 管理者のユーザー ID とパスワード。ユーザー ID 例: `admin`
Administration Server インスタンスへの HTTP または HTTPS アクセス	Administration Server インスタンスへの HTTP アクセスをセキュリティー保護するかどうかを指定する必要があります。

Java Enterprise System インストーラの実行

Java Enterprise System インストーラプログラムは、相互運用される一連の製品、共有コンポーネント、ライブラリをインストールします。

Delegated Administrator を正しくインストールし設定するには、Java Enterprise System インストーラを実行して次のコンポーネントをインストールする必要があります。

- Sun Java System Directory Server 5.x
- Sun Java System Access Manager 7.0

  Access Manager 7 には次の 2 つのインストールタイプがあります。旧バージョンモード (デフォルト) と レルムモードです。旧バージョンモードは Delegated Administrator と互換性があります。

Java Enterprise System インストーラを実行するときに、Access Manager の最初のパネルでインストールタイプとして旧バージョンモードを選択する必要があります。レルムモードを選択しないでください。

Delegated Administrator では LDAP Schema 2 を使用してユーザーとグループをプロビジョニングする必要があるため、Access Manager をインストールする必要があります。

- 次のいずれかの Web コンテナ
  - Sun Java System Web Server 6.1
  - Sun Java System Application Server 7.*x*
  - Sun Java System Application Server 8.*x*

    (Java Enterprise System インストーラは、Directory Server 5.x と上記の Web コンテナのいずれかがインストールされていることも確認します。)
- Sun Java System Messaging Server と Sun Java System Calendar Server のいずれか、または両方。

  Delegated Administrator は、Messaging Server と Calendar Server のプロビジョニングツールです。したがって、Delegated Administrator を正しく使用するには、これらのアプリケーションのいずれか、あるいは両方をインストールしてください。

  Messaging Server の設定手順については、『Sun Java System Messaging Server 管理ガイド』を参照してください。Calendar Server の設定手順については、『Sun Java System Calendar Server 管理ガイド』を参照してください。
- Delegated Administrator

  Java Enterprise System インストーラでは、Delegated Administrator をインストールするかどうかを確認するパネルが表示されます。このパネルで、Delegated Administrator をインストールすることを指定してください。

  (以前のリリースでは、Delegated Administrator は Access Manager とともに自動的にインストールされていました。)

  インストーラによって、Delegated Administrator が *da_base* で指定されたディレクトリ (たとえば、デフォルトは `/opt/SUNWcomm`) にインストールされます。

Java Enterprise System インストーラの詳細については、『 Sun Java Enterprise System インストールガイド』を参照してください。

注 – Delegated Administrator を以前の Sun Java System バージョンからアップグレードしている場合は、『Sun Java Enterprise System アップグレードと移行』の「Delegated Administrator のアップグレード」の章を参照してください。

Directory Server セットアップスクリプトの実行

Delegated Administrator、Messaging Server、または Calendar Server を設定する前に、Directory Server Preparation Tool スクリプト (`comm_dssetup.pl`) を実行する必要があります。`comm_dssetup.pl` スクリプトの実行は 1 回しか必要ありません。

このスクリプトは、Delegated Administrator、Messaging Server、または Calendar Server の構成で動作するように LDAP Directory Server の設定を変更します。`comm_dssetup.pl` スクリプトは、新しいスキーマ、インデックス、および設定データを設定することによって、Directory Server を準備します。

`comm_dssetup.pl` スクリプトの手順とオプションについては、『Sun Java System Messaging Server 管理ガイド』または『Sun Java System Calendar Server 管理ガイド』を参照してください。

Delegated Administrator を実行するには、`comm_dssetup.pl` スクリプトの実行時に「Schema 2」のスキーマタイプを選択する必要があります。

ディレクトリの ACI の統合

Access Manager、Messaging Server、LDAP Schema 2 ディレクトリと共に大規模なインストールを行うときは、ディレクトリ内の Access Control Instructions (ACI) を統合した方がよい場合があります。

Messaging Server と共に Access Manager をインストールすると、多数の ACI がディレクトリにインストールされます。デフォルトの ACI の多くは Messaging Server では使用しません。ディレクトリ内のデフォルト ACI の数を減らし統合すると Directory Server のパフォーマンスが向上し、その結果 Messaging Server のルックアップのパフォーマンスが向上します。

ACI を統合する方法、および使用していない ACI を削除する方法については、このガイドの後半にある 付録 E を参照してください。

Delegated Administrator の設定

Delegated Administrator のインストール後、47 ページの「Delegated Administrator 設定情報の収集」を参照して、Delegated Administrator 設定プログラムを実行してください。

設定プログラムの実行方法については、第 3 章を参照してください。

Messaging Server と Calendar Server の設定

Messaging Server の設定手順については、『Sun Java System Messaging Server 管理ガイド』を参照してください。Calendar Server の設定手順については、『Sun Java System Calendar Server 管理ガイド』を参照してください。

第 3 章

Delegated Administrator の設定

Delegated Administrator の設定プログラム (`config-commda`) は、個々の要件に従って基づき新しい設定を作成します。この最初の実行時設定プログラムでは、最小限の設定が行われます。

プログラムの実行後、76 ページの「設定後の作業」で説明する手順に従って初期設定を完了してください。

さらに、第 4 章で説明する作業を行い、Delegated Administrator の設定をカスタマイズできます。

『Sun Java System Messaging Server 管理ガイド』で説明しているように、追加設定が必要な場合があります。

この章では、次の項目を説明します。

以前のリリースの Delegated Administrator からアップグレードする場合

Delegated Administrator を初めて設定する場合、この項を省略して59 ページの「設定コンポーネントの選択」に進んでください。

以前の Java Enterprise System リリースからこのリリースの Delegated Administrator にアップグレードする場合、Delegated Administrator を設定する前に、次の作業が必要になる場合があります。

- 56 ページの「既存の設定の保存」
- 57 ページの「カスタマイズされたサービスパッケージのアップグレード」

Delegated Administrator を以前の Sun Java System バージョンからアップグレードする方法については、『Sun Java Enterprise System アップグレードガイド』の「Delegated Administrator のアップグレード」の章を参照してください。

既存の設定の保存

この項は、以前に Delegated Administrator をインストールおよび設定し、Delegated Administrator の設定をカスタマイズした場合のみ関係があります。

設定をカスタマイズした場合、Delegated Administrator 設定プログラム `config-commda` を再実行すると、設定ファイル内のプロパティーはデフォルト値にリセットされます。これらのファイルは、後述の56 ページの「Delegated Administrator プロパティーファイル」に記載されています。

Delegated Administrator のカスタマイズ方法については、第 4 章を参照してください。

Delegated Administrator をアップグレードする前、またはその他の理由で Delegated Administrator 設定プログラムを再実行する前に、カスタマイズした設定を保存してください。

Delegated Administrator プロパティーファイル

Delegated Administrator では、次のプロパティーファイルがインストールされます。

- `resource.properties`

  デフォルトの場所

  da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet`
- `daconfig.properties`

  デフォルトの場所

  da_base`/data/WEB-INF/classes/com/sun/comm/da/resources`
- `cli-usrprefs.properties`

  デフォルトの場所 `/var/opt/SUNWcomm/config`
- `security.properties`

  デフォルトの場所*da_base*`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

- `Resources.properties`

  デフォルトの場所

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`
- `logger.properties`

  デフォルトの場所

  da_base`/data/da/WEB-INF/classes/com/sun/comm/da/resources`

▼ 既存の設定を保存する

手順 **1.** カスタマイズしたプロパティーファイルをバックアップします。

プロパティーファイルとそのデフォルトの格納場所については、56 ページの「Delegated Administrator プロパティーファイル」を参照してください。

2. **`config-commda`** プログラムを実行します。実行方法については、この章の後半で説明します。

残りのステップでは、`resource.properties` ファイルを例として使用します。カスタマイズしたファイルごとに、これらのステップを繰り返します。

3. **`config-commda`** プログラムによって作成された新しい **`resource.properties`** ファイルを次のように編集します。

a. 新しい **`resource.properties`** ファイルを開きます。

b. **`resource.properties`** ファイルのバックアップコピーを開きます。

c. バックアップコピーでカスタマイズしたプロパティーを探します。カスタマイズした値を新しい **`resource.properties`** ファイル内の対応するプロパティーに適用します。

バックアップコピー全体で新しい `resource.properties` ファイルを単純に上書きしないでください。新しいファイルには、このリリースの Delegated Administrator をサポートするために作成された新しいプロパティーが含まれている可能性があります。

カスタマイズされたサービスパッケージのアップグレード

この項は、Communications Services 6 2005Q1 Delegated Administrator から Communications Services 6 2005Q4 Delegated Administrator へのアップグレードで、以前のリリース (6 2005Q1) でカスタマイズされたサービスパッケージを作成した場合のみ該当します。

現在のリリース (6 2005Q4) の Delegated Administrator では、サービスパッケージはユーザーまたはグループに対してカレンダサービスとメールサービスを提供することができます。以前のリリース (6 2005Q1) では、サービスパッケージが提供したのはユーザーに対するメールサービスだけでした。サービスパッケージの定義には、新しい機能をサポートする新しい属性が含まれています。

サンプルサービスクラステンプレート

Delegated Administrator 設定プログラムを実行すると、以前に Delegated Administrator 設定プログラムによってインストールされたサンプルサービスクラステンプレートは自動的にアップグレードされます。設定プログラムの「サービスパッケージと組織のサンプル」パネルで、「 サンプルサービスパッケージを読み込む」を選択してください。

サンプルテンプレートを使用してサービスパッケージをユーザーとグループに割り当てるだけであれば、操作は必要ありません。

カスタマイズされたサービスパッケージ

設定プログラムでは、6 2005Q1 リリースで作成したカスタマイズされたサービスパッケージはアップグレードされません。カスタマイズされたサービスパッケージは、手動でアップグレードする必要があります。

カスタマイズされたサービスパッケージの作成方法については、77 ページの「独自のサービスパッケージの作成」を参照してください。

▼ カスタマイズされたサービスパッケージをアップグレードする

手順 **1.** サービスパッケージを定義する **ldif** ファイルに次の行を追加して、カスタマイズされたサービスパッケージをそれぞれ編集します。

```
daServiceType: mail user
```

`daServiceType` 属性はサービスのタイプ (メールまたはカレンダ) およびターゲット (ユーザーまたはグループ) を定義します。

以前のリリースで作成されたサービスパッケージが提供するのは、ユーザーに対するメールサービスのみです。したがって、`daServiceType` の値は `mail user` にしてください。

編集済みの ldif ファイルの例を次に示します。

```
dn: cn=myservicepackage,o=cosTemplates,o=mycompanysuffix
changetype: modify
replace: daServiceType
daServiceType: mail user
```

2. **LDAP** ディレクトリツール **`ldapmodify`** を使用して、ディレクトリ内のサービスパッケージを更新します。

   コマンド実行の例を次に示します。

   ```
   ldapmodify -D <directory manager> -w <password> -f
   myservicepackage
   ```

   各表記の意味は次のとおりです。

   `<directory manager>` は Directory Server 管理者の名前です。

   `<password>` は Directory Service 管理者のパスワードです。

   `myservicepackage` はカスタマイズされたサービスパッケージを定義する ldif ファイルの名前です。

設定コンポーネントの選択

設定プログラムの 3 番目のパネルでは、設定が必要な Delegated Administrator コンポーネントの指定が要求されます。

- **Delegated Administrator** ユーティリティー **(**クライアント**)** — `commadmin` で呼び出されるコマンド行インタフェース。
- **Delegated Administrator** サーバー — Delegated Administrator のユーティリティーとコンソールを実行するのに必要な Delegated Administrator サーバーコンポーネント。
- **Delegated Administrator** コンソール — Delegated Administrator グラフィカルユーザーインタフェース (GUI)。

選択したコンポーネントに応じて、設定プログラムで表示されるパネルは異なります。

次のステップに設定の選択肢をまとめています。後述の要約された各ステップは、以降の特定の項にリンクし、各項で実際の設定パネルを説明していきます。

▼ 設定の種類の要約

手順 **1.** 61 ページの「設定の開始」
パネルで要求される情報を入力し、設定を開始します。

2. 63 ページの「**Delegated Administrator** ユーティリティーの設定」
このステップ内のパネルは、「設定するコンポーネントを選択」パネルに続いて表示されます。パネルでは、Delegated Administrator ユーティリティーの設定に使用される情報の入力が要求されます。

Delegated Administrator ユーティリティーは必須であり、Delegated Administrator コンポーネント (サーバーまたはコンソール) をインストールするすべてのマシンで設定する必要があります。

したがって、常にこれらのパネルへの情報入力が必要になります。

3. 64 ページの「**Delegated Administrator** コンソールの設定」
このステップ内のパネルは、ユーティリティー設定パネルに続いて表示されます。

Delegated Administrator コンソールを設定するかどうかを選択できます。

- 同じマシンに Delegated Administrator のコンソールとサーバーを配備する場合、「設定するコンポーネントを選択」パネルでコンソールとサーバーを選択します。
- また Delegated Administrator のコンソールとサーバーを別のマシンに配備することもできます。

  コンソールを配備するマシンでは、コンソールは「設定するコンポーネントを選択」パネルからのみ選択できますこのユーティリティーは常に選択されています。

  この場合、サーバーを配備するマシンで、再び設定プログラムを実行する必要があります。

  コンソールとサーバーを異なるマシンに配備する場合、このユーティリティーはいずれのマシンにも設定されます。

コンソールに選択した Web コンテナに応じて、設定プログラムで表示されるパネルは異なります。次の Web コンテナのいずれかに配備できます。

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

1 台のマシンで Delegated Administrator のサーバーとコンソールを設定する場合、説明する手順を 2 回 (サーバーとコンソールに 1 回ずつ) 実行します。

4. 69 ページの「**Delegated Administrator** サーバーの設定」
このステップ内のパネルは、コンソール設定パネルに続いて表示されます。

特定のマシンに Delegated Administrator サーバーを設定するかどうかを選択できます。

特定のマシンにサーバーを設定しない場合、設定プログラムから別のマシンにサーバーを設定するように警告されます。サーバーコンポーネントは、ユーティリティーとコンソールの実行に必要です。

サーバーの配備に必要となるその他すべての注意事項は、64 ページの「Delegated Administrator コンソールの設定」で説明するコンソールに関する注意事項と同じです。

また、サーバーは Access Manager と同じ Web コンテナを使用することに注意してください。設定プログラムは Access Manager 基本ディレクトリの設定を要求したあと、Web コンテナ情報の入力を要求します。

5. 72 ページの「設定の完了」
   これらのパネルで要求される情報を入力し、設定を終了します。

設定プログラムの実行

この項で説明するステップに従って、Delegated Administrator を設定します。

設定プログラムの起動

設定プログラムを実行するには、ルートでログインするか、またはルートになって `/opt/SUNWcomm/sbin` ディレクトリに進みます。そのあとに、次のコマンドを入力します。

```
# ./config-commda
```

`config-commda` コマンドを実行すると、設定プログラムが起動します。

以降の項では、設定パネルについて順番に説明しています。

設定の開始

設定プログラムの最初のパネルで要求される情報を入力する必要があります。

▼ 設定を開始する

手順 **1.** ようこそ

設定プログラムの最初のパネルは、著作権ページです。「 次へ」をクリックして続行するか、「取消し」をクリックして終了します。

2. 設定およびデータファイルを保存するディレクトリの選択

Delegated Administrator の設定およびデータファイルを保存するディレクトリを選択してください。デフォルト設定ディレクトリは `/var/opt/SUNWcomm` です。このディレクトリは、*da_base* ディレクトリ (`/opt/SUNWcomm`) と区別する必要があります。

ディレクトリ名を入力するかデフォルトをそのまま使い、「次へ」をクリックして作業を続けます。

ディレクトリが存在しない場合、ディレクトリを作成するか、新しいディレクトリを選択するか指定を要求するダイアログが表示されます。「ディレクトリを作成」をクリックしてディレクトリを作成するか、「新規に選択し直す」をクリックして新規ディレクトリを入力します。

コンポーネントのロード中を示すダイアログが表示されます。コンポーネントの読み込みには数分かかることがあります。

3. 設定するコンポーネントの選択

コンポーネントパネルで、設定する 1 つまたは複数のコンポーネントを選択します。

- **Delegated Administrator** ユーティリティー **(**クライアント**)** — `commadmin` で呼び出されるコマンド行インタフェース。このコンポーネントは必須であり、デフォルトで選択されます。選択の解除はできません。
- **Delegated Administrator Server** — Delegated Administrator コンソールを実行するのに必要な Delegated Administrator サーバーコンポーネント。
- **Delegated Administrator** コンソール — Delegated Administrator グラフィカルユーザーインタフェース (GUI)。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

コンポーネントの選択方法については、59 ページの「設定コンポーネントの選択」を参照してください。

Delegated Administrator サーバーを設定しない場合、Delegated Administrator サーバーを別のマシンで設定するように注意するダイアログボックスが表示されます。サーバーを設定し、Delegated Administrator のユーティリティーとコンソールの動作を有効にする必要があります。

Delegated Administrator ユーティリティーの設定

Delegated Administrator コンポーネント (サーバーまたはコンソール) をインストールしたすべてのマシンで Delegated Administrator ユーティリティーを設定する必要があります。

▼ Delegated Administrator ユーティリティーを設定する

手順

1. **Access Manager** のホスト名とポート番号

   Access Manager (以前の Identity Server) のホスト名とポート番号を入力します。Delegated Administrator サーバーコンポーネントをインストールする場合、Access Manager と同じホストにインストールする必要があります。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

2. デフォルトドメイン

   最上位管理者のデフォルトドメインを入力します。`commadmin` コマンド行ユーティリティーを実行する場合に、ドメインが `-n` オプションにより明示的に指定されないときに使用されるドメインです。これはデフォルト組織として知られます。指定したドメインがディレクトリに存在しない場合、作成されます。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

3. クライアントのデフォルト **SSL** ポート

   Delegated Administrator ユーティリティーが使用するデフォルト SSL ポートを入力します。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

4. **Delegated Administrator** ユーティリティーのみを設定する場合、次の項目に進みます。

   72 ページの「設定の完了」

   Delegated Administrator コンソールとサーバーの両方を設定する場合、またはコンソールのみを設定する場合、次の項目に進みます。

   64 ページの「Delegated Administrator コンソールの設定」

   Delegated Administrator サーバーおよび必須 Delegated Administrator ユーティリティーのみを設定する場合、次の項目に進みます。

   69 ページの「Delegated Administrator サーバーの設定」

Delegated Administrator コンソールの設定

設定プログラムには、次のパネルが表示されます。

Delegated Administrator の **Web** コンテナを選択

Delegated Administrator コンソールを配備する Web コンテナを選択します。Delegated Administrator は次のプラットフォームに設定できます。

- Sun Java System Web Server
- Sun Java System Application Server 7.*x*
- Sun Java System Application Server 8.*x*

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

このパネルと以降のパネルは、Delegated Administrator コンソールの Web コンテナに関する情報を収集します。該当する項の指示に従ってください。

- 64 ページの「Web Server の設定」
- 66 ページの「Application Server 7.*x* の設定」
- 67 ページの「Application Server 8.*x* の設定」

Delegated Administrator のコンソールとサーバーは、2 つの異なる Web コンテナ、Web コンテナの 2 つの異なるインスタンス、または同じ Web コンテナに配備できます。

パネル 3 で、Delegated Administrator コンソールと Delegated Administrator サーバーを設定する場合、2 番目に表示される一連のパネルで、サーバーの Web コンテナに関する情報の指定が要求されます。

この場合、Web コンテナの設定パネルが 2 度表示されます。Delegated Administrator の各コンポーネントを配備するための指示に従います。

Web コンテナの設定パネルを終了する際、次の手順に従います。

- Delegated Administrator コンソールとサーバーの両方を設定する場合、次の項目に進みます。

  69 ページの「Delegated Administrator サーバーの設定」
- Delegated Administrator コンソールおよび必須 Delegated Administrator ユーティリティーのみを設定する場合、次の項目に進みます。

  72 ページの「設定の完了」

Web Server の設定

Web Server に Delegated Administrator サーバーまたはコンソールを配備する場合、この項で説明するステップに従います。

▼ Web Server を設定する

手順 **1. Web Server** の設定の詳細

Delegated Administrator のサーバー用またはコンソール用に Web Server の設定情報を設定するかどうか、パネルテキストを参照してください。

Web Server ルートディレクトリを入力します。ディレクトリを参照して選択できます。

Web Server インスタンス識別子を入力します。これは `west.sesta.com` などの *host.domain* 名で指定できます。

仮想サーバー識別子を入力します。これは `https-west.sesta.com` などの `https-` *host.domain* 名で指定できます。

Web Server インスタンス識別子と仮想サーバー識別子の詳細については、Web Server のマニュアルを参照してください。

Web Server インスタンスのファイルは、`/opt/SUNWwbsvr/https-west.sesta.com` など、Web Server インストールディレクトリ内の `https-`*host* `.`*domain* ディレクトリに格納されます。

Web Server の HTTP ポート番号を入力します。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

設定プログラムは、指定した値が有効かどうかを確認します。ディレクトリまたは識別子が無効か、存在しない場合、新しい値の選択を指示するダイアログが表示されます。

次に、設定プログラムは、Web Server インスタンス接続が稼働中かどうかを確認します。稼働していない場合、設定プログラムが指定されたインスタンスに接続できず、設定が終了しない場合があることがダイアログボックスで警告されます。指定された値を使用するか、新しい Web Server 設定値を選択します。

2. デフォルトのドメイン区切り文字

このパネルが表示されるのは、Delegated Administrator コンソールを設定する場合のみです。ドメイン区切り文字は、コンソールの設定に必要になります。 この情報は Web コンテナとは関係がありません。

ログオン時の認証に使用するデフォルトのドメイン区切り文字を入力します。例 : `@`

ドメイン区切り文字の値は、`daconfig.properties` ファイル内にあります。プログラムの実行後に、このプロパティー値を変更できます。詳細については、第 4 章を参照してください。

3. Delegated Administrator コンソールを設定する場合、次の手順に従います。

- Delegated Administrator コンソールとサーバーの両方を設定する場合、次の項目に進みます。

  69 ページの「Delegated Administrator サーバーの設定」
- Delegated Administrator コンソールおよび必須 Delegated Administrator ユーティリティーのみを設定する場合、次の項目に進みます。

  72 ページの「設定の完了」

Delegated Administrator サーバーを設定する場合、次の手順に従います。

次の項目に進みます。

69 ページの「Delegated Administrator サーバーの設定」の手順 3。

Application Server 7.*x* の設定

Application Server 7.*x* に Delegated Administrator のサーバーまたはコンソールを配備する場合、この項で説明するステップに従います。

▼ Application Server 7.*x* を設定する

手順 **1. Application Server 7.*x*** の設定の詳細

Delegated Administrator のサーバー用またはコンソール用の Application Server 7.*x* の設定情報を指定するかどうか、パネルテキストを参照してください。

Application Server インストールディレクトリを入力します。デフォルトでは、このディレクトリは `/opt/SUNWappserver7` になります。

Application Server ドメインディレクトリを入力します。デフォルトでは、このディレクトリは `/var/opt/SUNWappserver7/domains/domain1` になります。

Application Server ドキュメントルートディレクトリを入力します。デフォルトでは、このディレクトリは `/var/opt/SUNWappserver7/domains/domain1/server1/docroot` になります。

ディレクトリのいずれかを参照して選択します。

Application Server インスタンス名を入力します。例 : `server1`

Application Server 仮想サーバー識別子を入力します。例 : `server1`

Application Server インスタンスの HTTP ポート番号を入力します。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

設定プログラムは、指定した値が有効かどうかを確認します。ディレクトリが無効か存在しない場合、新しいディレクトリの選択を指示するダイアログが表示されます。

次に、設定プログラムは、Application Server インスタンス接続が稼働中かどうかを確認します。稼働していない場合、設定プログラムが指定されたインスタンスに接続できず、設定が終了しない場合があることがダイアログボックスで警告されます。指定された値を使用するか、新しい Application Server 設定値を選択します。

2. **Application Server 7.x:**管理インスタンスの詳細

   管理サーバーのポート番号を入力します。例 : `4848`

   管理サーバーの管理者ユーザー ID を入力します。例 : `admin`

   管理者のユーザーパスワードを入力します。

   安全な Administration Server インスタンスを使用する場合、「セキュリティー保護された管理サーバーインスタンス」のチェックボックスを選択します。使用しない場合、チェックボックスのチェックを外します。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

3. デフォルトのドメイン区切り文字

   このパネルが表示されるのは、Delegated Administrator コンソールを設定する場合のみです。ドメイン区切り文字は、コンソールの設定に必要になります。 この情報は Web コンテナとは関係がありません。

   ログオン時の認証に使用するデフォルトのドメイン区切り文字を入力します。例 : `@`

4. **Delegated Administrator** コンソールを設定する場合、次の手順に従います。

   - Delegated Administrator コンソールとサーバーの両方を設定する場合、次の項目に進みます。

     69 ページの「Delegated Administrator サーバーの設定」

   - Delegated Administrator コンソールおよび必須 Delegated Administrator ユーティリティのみを設定する場合、次の項目に進みます。

     72 ページの「設定の完了」

   Delegated Administrator サーバーを設定する場合、次の手順に従います。

   次の項目に進みます。

   69 ページの「Delegated Administrator サーバーの設定」の手順 3。

Application Server 8.*x* の設定

Application Server 8.*x* に Delegated Administrator のサーバーまたはコンソールを配備する場合、次の手順に従います。

▼ Application Server 8.*x* を設定する

手順 **1. Application Server 8.x** の設定の詳細

Delegated Administrator のサーバー用またはコンソール用の Application Server 8.*x* の設定情報を指定するかどうか、パネルテキストを参照してください。

Application Server インストールディレクトリを入力します。デフォルトでは、このディレクトリは `/opt/SUNWappserver/appserver` になります。

Application Server ドメインディレクトリを入力します。デフォルトでは、このディレクトリは `/var/opt/SUNWappserver/domains/domain1` になります。

Application Server ドキュメントルートディレクトリを入力します。デフォルトでは、このディレクトリは `/var/opt/SUNWappserver/domains/domain1/docroot` になります。

ディレクトリのいずれかを参照して選択します。

Application Server ターゲット名を入力します。例 : `server`

Application Server 仮想サーバー識別子を入力します。例 : `server`

Application Server ターゲット HTTP ポート番号を入力します。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

設定プログラムは、指定した値が有効かどうかを確認します。ディレクトリが無効か存在しない場合、新しいディレクトリの選択を指示するダイアログが表示されます。

次に、設定プログラムは、Application Server ターゲット接続が稼働中かどうかを確認します。稼働していない場合、設定プログラムが指定されたターゲットに接続できず、設定が終了しない場合があることがダイアログボックスで警告されます。指定された値を使用するか、新しい Application Server 設定値を選択します。

2. Application Server 8.x:管理インスタンスの詳細

管理サーバーのポート番号を入力します。例 : `4849`

管理サーバーの管理者ユーザー ID を入力します。例 : `admin`

管理者のユーザーパスワードを入力します。

安全な Administration Server インスタンスを使用する場合、「セキュリティー保護された管理サーバーインスタンス」のチェックボックスを選択します。使用しない場合、チェックボックスのチェックを外します。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルに戻るか、または「取消し」をクリックして終了します。

3. デフォルトのドメイン区切り文字

   このパネルが表示されるのは、Delegated Administrator コンソールを設定する場合のみです。ドメイン区切り文字は、コンソールの設定に必要になります。 この情報は Web コンテナとは関係がありません。

   ログオン時の認証に使用するデフォルトのドメイン区切り文字を入力します。例 : @

4. **Delegated Administrator** コンソールを設定する場合、次の手順に従います。

   - Delegated Administrator コンソールとサーバーの両方を設定する場合、次の項目に進みます。

     69 ページの「Delegated Administrator サーバーの設定」
   - Delegated Administrator コンソールおよび必須 Delegated Administrator ユーティリティーのみを設定する場合、次の項目に進みます。

     72 ページの「設定の完了」

   Delegated Administrator サーバーを設定する場合、次の手順に従います。

   次の項目に進みます。

   69 ページの「Delegated Administrator サーバーの設定」の手順 3。

Delegated Administrator サーバーの設定

Delegated Administrator サーバーの設定を選択した場合、設定プログラムには次のパネルが表示されます。

▼ Delegated Administrator サーバーを設定する

手順 1. **Access Manager** ベースディレクトリ

   Access Manager ベースディレクトリを入力します。デフォルトディレクトリは `/opt/SUNWam` です。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

   設定プログラムは、有効な Access Manager ベースディレクトリが指定されているかどうかを確認します。指定されていない場合、既存の Access Manager ベースディレクトリの選択を指示するダイアログボックスが表示されます。

2. 次に、**Web** コンテナの「設定の詳細」パネルが表示されます。

   コンソールとサーバーを設定する場合、この Web コンテナの「設定の詳細」パネルが表示されるのは 2 度目です。

Delegated Administrator サーバーは、Access Manager と同じ Web コンテナに配備されます。Delegated Administrator サーバーには Web コンテナを選択できません。

該当する項の指示に従ってください。

- 64 ページの「Web Server の設定」
- 66 ページの「Application Server 7.*x* の設定」
- 67 ページの「Application Server 8.*x* の設定」

3. ディレクトリ **(LDAP)** サーバー

   このパネルでは、ユーザー/グループのサフィックスに対する LDAP ディレクトリサーバーへの接続に関する情報が要求されます。

   各テキストボックスにユーザーおよびグループの Directory Server LDAP URL (**LdapURL**)、Directory Manager (バインド)、およびパスワードを入力します。

   ディレクトリマネージャーには、ディレクトリサーバー、およびディレクトリサーバーを使用するすべての Sun Java System サーバー (Delegated Administrator など) に対する包括的な管理権限が付与されており、ディレクトリサーバー内のすべてのエントリに対する完全な管理アクセス権が与えられています。推奨されるデフォルトの識別名 (DN) は `cn=Directory Manager` です。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

4. **Access Manager** 最上位管理者

   Access Manager 最上位管理者のユーザー ID とパスワードを入力します。ユーザー ID とパスワードは、Access Manager のインストール時に作成されます。デフォルトユーザー ID は `amadmin` です。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

5. **Access Manager** 内部 **LDAP** 認証パスワード

   Access Manager 内部 LDAP 認証ユーザーのパスワードを入力します。

   認証ユーザー名は、`amldapuser` としてハードコードされています。認証ユーザー名は Access Manager インストーラで作成され、LDAP サービスのバインド DN ユーザーです。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

6. 組織識別名 **(DN)**

   デフォルトドメインの組織 DN を入力します。たとえば、組織 DN が `o=siroe.com` であれば、その組織内のすべてのユーザーは LDAP DN `o=siroe.com, o=usergroup` 内に置かれます。`o=usergroup` はルートサフィックスです。

デフォルトでは、設定プログラムは LDAP ディレクトリ内のルートサフィックスの下にデフォルトドメインを追加します。

ルートサフィックスの下ではなく、ルートサフィックスと同じレベルでデフォルトドメインを作成する場合、「組織 **DN**」テキストボックスに表示される DN から組織名を削除します。

たとえば、組織 DN が `o=siroe.com` でルートサフィックスが `o=usergroup` であれば、テキストボックスの DN から "`o=siroe.com`" を削除し、`o=usergroup` のみを残します。

ルートサッフィクスでデフォルトドメインを作成すると、あとでホストドメインを使用するときに、ホストドメインの設定に移行するのが難しい場合があります。`config-commda` プログラムによって次の警告が表示されます。

「選択された組織 DN はユーザー/グループサフィックスです。これは有効な選択ですが、ホストされたドメインを使用することにした場合、移行に関する複雑な問題が発生します。ホストされたドメインを使用する場合は、DN をユーザー/グループサフィックスより 1 レベル下に指定してください。」

詳細については、28 ページの「単層階層をサポートするディレクトリ構造」を参照してください。

「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

7. デフォルト組織の最上位管理者

   デフォルトドメインで作成される最上位管理者のユーザー ID とパスワードを入力します。

   「パスワードの確認」フィールドに再度パスワードを入力します。

   「次へ」をクリックして続行するか、「戻る」をクリックして前のパネルへ戻るか、または「取消し」をクリックして終了します。

8. サービスパッケージと組織サンプル

   サンプルサービスパッケージとサンプル組織を、LDAP ディレクトリに追加できます。

   「サンプルサービスパッケージを読み込む」。サンプルサービスパッケージテンプレートを使用または変更して、独自のサービスクラスパッケージを作成する場合、このオプションを選択します。

   「サンプル組織を読み込む」。LDAP ディレクトリツリーにサンプルプロバイダ組織ノードと下位組織ノードを含める場合、このオプションを選択します。

   次のいずれかを選択できます。

   - サンプルサービスパッケージとサンプル組織の両方
   - オプションのいずれか
   - オプションをどれも選択しない

「サンプル用の優先メールホスト」。Messaging Server がインストールされているマシンの名前を入力します。

例 : `mymachine.siroe.com`

LDAP ディレクトリにサンプル組織をロードする場合、これらのサンプルの優先メールホスト名を入力する必要があります。

サービスパッケージと組織の詳細については、第 2 章「Delegated Administrator の概要」を参照してください。

設定プログラムを実行したあと、サービスパッケージテンプレートを変更し、独自のサービスクラスパッケージを作成します。この設定後の作業については、77 ページの「サービスパッケージの作成」を参照してください。

設定の完了

設定プログラムの実行を終了するには、この項に説明する手順に従います。

▼ 設定を完了する

手順 **1.** 設定準備完了

確認パネルに、設定される項目が表示されます。

「すぐに設定」をクリックして設定を開始するか、「戻る」をクリックして前のパネルに戻り情報を変更するか、または「取消し」をクリックして終了します。

2. タスクシーケンス

実行する作業の順序は、「タスクシーケンス」パネルに表示されます。このときに実際の設定作業を実行されます。

パネルに「すべてのタスクが成功しました」のメッセージが表示されたら、「次へ」をクリックして作業を続けるか、「取消し」をクリックして作業の実行を停止して終了します。

設定変更を有効にするために Web コンテナの再起動を要求するダイアログボックスが表示されます。

3. インストールの概要

「インストールの要約」パネルには、インストールされた製品と、この設定に関する詳細情報を示した「詳細...」ボタンが表示されます。

`config-commda` プログラムのログファイルは、`/opt/SUNWcomm/install` ディレクトリ内に作成されます。ログファイル名は、`commda-config_`*YYYYMMDDHHMMSS*`.log` です。 *YYYYMMDDHHMMSS* は設定の 4 桁の年、月、日、時間、分、秒を表します。

「閉じる」をクリックして設定を終了します。

Web コンテナの再起動

Delegated Administrator の設定が完了したら、Delegated Administrator が配備されている次のいずれかの Web コンテナを再起動する必要があります。

- Web Server
- Application Server 7.x
- Application Server 8.x

config-commda プログラムで作成された設定ファイルとログファイル

設定ファイル

各パネルに指定した情報に基づき、config-commda プログラムは 3 つの Delegated Administrator コンポーネントに次の設定ファイルを作成します。

- Delegated Administrator ユーティリティー

  設定ファイル名: cli-usrprefs.properties

  デフォルトの場所/var/opt/SUNWcomm/config
- Delegated Administrator サーバー

  設定ファイル名: resource.properties

  デフォルトの場所

  /opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet

  または

  /var/opt/SUNWcomm/WEB-INF/classes/sun/comm/cli/server/servlet
- Delegated Administrator コンソール

  設定ファイル名: daconfig.properties

  デフォルトの場所

  /opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources

  または

  /var/opt/SUNWcomm/WEB-INF/classes/com/sun/comm/da/resources

これらのファイルと、ファイル内のプロパティー、およびプロパティーを編集して設定をカスタマイズする方法については、第 4 章を参照してください。

ログファイル

Delegated Administrator コンソールは、次の実行時ログファイルを作成します。

デフォルトログファイル名: `da.log`

デフォルトの場所`/opt/SUNWcomm/log`

Delegated Administrator の実行時ログファイルとその他のログファイルについては、付録 C を参照してください。

サイレントインストールの実行

Delegated Administrator ユーティリティーの初期実行時設定プログラムは、`saveState` というサイレントインストールの状態ファイルを自動的に作成します。このファイルには、設定プログラムに関する内部情報が収められ、サイレントインストールの実行に使用されます。

`saveState` サイレントインストールファイルは `/opt/SUNWcomm/data/setup/commda-config_`*YYYYMMDDHHMMSS* `/` ディレクトリに保存されます。*YYYYMMDDHHMMSS* は、`saveState` ファイルの 4 桁の年、月、日、時、分、および秒を示します。

たとえば、`config-commda` プログラムを 1 度実行すると、サイレントインストールモードでプログラムを実行できます。

```
da_base/sbin/config-commda -nodisplay -noconsole -state
 fullpath/saveState
```

fullpath 変数は `saveState` ファイルが置かれている完全ディレクトリパスです。

Delegated Administrator コンソールとユーティリティーの実行

コンソールの起動

Delegated Administrator コンソールは、コンソールが配備されている Web コンテナにアクセスすることで起動されます。

▼ Delegated Administrator コンソールを起動する

手順 **1.** 次の **URL** に進みます。

`http://` *host*`:`*port*`/da/DA/Login`

各表記の意味は次のとおりです。

host は Web コンテナのホストマシンです。

port は Web コンテナのポートです。

例 :

```
http://siroe.com:8080/da/DA/Login
```

Delegated Administrator コンソールのログインウインドウが表示されます。

2. **Delegated Administrator** コンソールにログインします。

Delegated Administrator 設定プログラムで指定した最上位管理者 (TLA) のユーザー ID とパスワードを使用します。この情報は、次のパネルで要求されたものです。

デフォルト組織の「最上位管理者」

注 – Delegated Administrator コンソールの実行中は、Access Manager で設定された値によってセッションタイムアウトが判断されます。セッションタイムアウト値の詳細については、『*Sun Java System Access Manager* 管理ガイド』の「セッションサービス属性」を参照してください。セッションタイムアウト値を Access Manager コンソールで確認する方法については、『*Sun Java System Access Manager* 管理ガイド』の「現在のセッション」を参照してください。

コマンド行ユーティリティーの実行

Delegated Administrator ユーティリティーを実行するには、ターミナルウィンドウからコマンド名「`commadmin`」を入力します。

▼ コマンド行ユーティリティーを実行する

手順 **1.** *da_base***`/bin/`** ディレクトリに進みます。たとえば、**`/opt/SUNWcomm/bin/`** です。

2. **`commadmin`** コマンドを入力します。

例 3–1 commadmin を使用したユーザーの検索

次のコマンドでは、varrius.com ドメインのユーザーが検索されます。

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

この commadmin コマンドの詳細については、138 ページの「commadmin user search」を参照してください。

参考 commadmin のリターンコード

ヒント – commadmin の処理に成功すると、コマンド行に OK のメッセージが表示されます。

失敗した場合は、次のメッセージが表示されます。

```
FAIL
```

<message>

<message> にはエラーテキストが表示されます。

設定後の作業

Delegated Administrator 設定プログラムを実行したあとは、次の作業を行います。

- 76 ページの「デフォルトドメインへのメールサービスとカレンダサービスの追加」
- 77 ページの「サービスパッケージの作成」

次の作業を実行するのは、Schema 2 互換モードで LDAP ディレクトリを使用している場合のみです。

- 82 ページの「Schema 2 互換モードの ACI の追加」

デフォルトドメインへのメールサービスとカレンダサービスの追加

config-commda プログラムはデフォルトドメインを作成します。

メールサービスまたはカレンダサービスを持つユーザーをデフォルトドメインに作成する場合は、最初にメールサービスとカレンダサービスをドメインに追加する必要があります。

これは、commadmin domain modify コマンドおよびそのオプション -S mail と -S cal を使って行います。

次の例は、commadmin domain modify を使ってデフォルトドメインにメールサービスとカレンダサービスを追加する方法を示しています。

```
commadmin domain modify -D chris -w bolton -n sesta.com -d siroe.com
 -S mail,cal -H test.siroe.com
```

commadmin コマンドの構文と詳細については、第 5 章を参照してください。

サービスパッケージの作成

Delegated Administrator で LDAP ディレクトリにプロビジョニングされた各ユーザーと各グループがサービスパッケージを保有するようにしてください。ユーザーまたはグループは複数のサービスパッケージを保有できます。

定義済みサービスクラステンプレート

Delegated Administrator 設定プログラム (config-commda) の実行時には、config-commda プログラムでサービスクラスのサンプルテンプレートをディレクトリにインストールするよう選択できます。

サービスクラスのサンプルテンプレートとサービスパッケージで使用できるメール属性については、第 1 章の 32 ページの「サービスパッケージ」を参照してください。

サービスクラスのサンプルテンプレートを使用すると、サービスパッケージを作成し割り当てることができます。ただし、サンプルテンプレートはあくまでも例です。

独自のサービスパッケージの作成

通常、カスタマイズされたサービスクラステンプレートを基に、インストールされた環境のユーザーとグループに適切な属性値を使用して独自のサービスパッケージを作成します。

独自のサービスパッケージを作成するには、da.cos.skeleton.ldif ファイルに保存されているサービスクラステンプレートを使用します。

このファイルは、カスタマイズされたサービスクラステンプレートを記述するためのテンプレートとして使用するために特別に作成されました。Delegated Administrator を設定するときには、このファイルは LDAP ディレクトリにインストールされません。

da.cos.skeleton.ldif ファイルにはパラメータ設定された 4 つのテンプレートが含まれます。それぞれが Delegated Administrator によって提供されるサービスクラス定義に対応しています。

- standardUserMail
- standardUserCalendar
- standardUserMailCalendar
- standardGroupMail

da.cos.skeleton.ldif ファイル内のパラメータ設定されたテンプレートを 1 つ以上使用して、独自のサービスクラステンプレートを作成できます。

da.cos.skeleton.ldif ファイルのサービスクラステンプレートを次に示します。

```
# Templates for creating COS templates for service packages.
#
# There are four COS definitions :
#   standardUserMail
#   standardUserCalendar
#   standardUserMailCalendar
#   standardGroupMail
#
# Each definition can have zero or more COS templates which
# define specific values for the attributes listed in the
# COS definition.
#
# Each COS definition points to a corresponding subdirectory
# in which COS templates for that definition (and no other
# definition) are found.  The templates directory structure
# is as follows:
# standardUserMail          => o=mailuser,o=costemplates,<ugldapbasedn>
# standardUserCalendar      => o=calendaruser,o=costemplates,
#                              <ugldapbasedn>
# standardUserMailCalendar  => o=mailcalendaruser,o=costemplates,
#                              <ugldapbasedn>
# standardGroupMail          => o=mailgroup,o=costemplates,
#                              <ugldapbasedn>
#
# Thus, all COS templates for the user mail service are found in the
# o=mailuser,o=costemplates,<ugldapbasedn> directory, etc.
#
# It is not necessary to have any templates for a given definition.
# In that case default values are assumed for those attributes defined
# in the COS definition.
#
# If a template is created for a definition there should be at least
# one attribute with a defined value.
#
# Consult documentation for values for the attributes.
# Documentation includes units and default values.
#
# The finished COS derived from this skeleton is added to the
# directory with the following command:
#
# ldapmodify -D <directory manager> -w <password>
# -f <cos.finished.template.ldif>
#
#
################################################################
```

```
#
#    standardMailUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailuser,o=cosTemplates,<rootSuffix>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailQuota: <ma:ilQuotaValue>
mailMsgQuota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
#
#
################################################################
#
#    standardCalendarUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - icsPreferredHost
# - icsDWPHost
# - icsFirstDay
#
dn: cn=<service package name>,o=calendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
icsPreferredHost: <preferredHostValue>
icsDWPHost: <dwpHostValue>
icsFirstDay: <firstDayValue>
daServiceType: calendar user
#
#
################################################################
#
#    standardMailCalendarUser COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
# - mailQuota
```

```
# - mailMsgQuota
# - mailAllowedServiceAccess
#
dn: cn=<service package name>,o=mailcalendaruser,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
mailquota: <mailQuotaValue>
mailmsgquota: <mailMsgQuotaValue>
mailAllowedServiceAccess: <mailAllowedServiceAccessValue>
daServiceType: calendar user
daServiceType: mail user
#
#
################################################################
#
#    standardMailGroup COS template
#
################################################################
# There must be a least one of the following attributes:
# - mailMsgMaxBlocks
#
#
dn: cn=<service package name>,o=mailgroup,o=cosTemplates,
    <ugldapbasedn>
changetype: add
objectclass: top
objectclass: LDAPsubentry
objectclass: extensibleobject
objectclass: cosTemplate
cn: <service package name>
mailMsgMaxBlocks: <mailMsgMaxBlocksValue>
daServiceType: mail group
```

▼ 独自のサービスパッケージを作成する

手順 **1. `da.cos.skeleton.ldif` ファイル内のいずれかのパラメータ設定済みテンプレートをコピーし、名前を変更します。**

Delegated Administrator をインストールすると、`da.cos.skeleton.ldif` ファイルが次のディレクトリにインストールされます。

da_base`/lib/config-templates`

次の `da.cos.skeleton.ldif` ファイル内のテンプレートから 1 つを選択し、コピーして名前を変更します。

```
standardUserMail
standardUserCalendar
```

```
standardUserMailCalendar
standardGroupMail
```

2. コピーしたテンプレートで、次のパラメータを編集します。

   - `<ugldapbasedn>`

     ルートサフィックスパラメータ `<rootSuffix>` を `o=usergroup` などに変更します。

     `<ugldapbasedn>` パラメータは DN に表示されます。

   - `<service package name>`

     `<service package name>` パラメータを独自のサービスパッケージ名に変更します。

     `<service package name>` パラメータは DN と `cn` に表示されます。

   - メール属性値

     ```
     <mailMsgMaxBlocksValue>
     <mailQuotaValue>
     <mailMsgQuotaValue>
     <mailAllowedServiceAccessValue>
     ```

     ユーザーの指定に従って値を編集します。

     たとえば、次のようなメール属性の値を入力します。

     ```
     mailMsgMaxBlocks: 400
     mailQuota: 400000000
     mailMsgQuota: 5000
     mailAllowedServiceAccess: imap:ALL$+pop:ALL$+smtp:ALL$+http:ALL
     ```

   - カレンダ属性値

     ```
     <preferredHostValue>
     <dwpHostValue>
     <firstDayValue>
     ```

     これらのパラメータは、`icsPreferredHost`、 `icsDWPHost`、および `icsFirstDay` の各 LDAP 属性の値を表します。

     ユーザーの指定に従って値を編集します。

   これらの属性の定義と詳細については、『*Sun Java System Communications Services Schema Reference*』の第 3 章「Messaging Server and Calendar Server Attributes」を参照してください。

   カスタマイズされたサービスクラステンプレートでは少なくとも 1 つの属性を使用する必要があります。カスタムテンプレートで 4 つすべてのメール属性を使用する必要はありません。サービスパッケージから 1 つまたは複数の属性を削除できます。

3. **LDAP** ディレクトリツール **`ldapmodify`** を使用して、サービスパッケージをディレクトリにインストールします。

   コマンド実行の例を次に示します。

```
ldapmodify -D <directory manager> -w <password> -f
<cos.finished.template.ldif>
```

各表記の意味は次のとおりです。

<directory manager> は Directory Server 管理者の名前です。

<password> は Directory Service 管理者のパスワードです。

<cos.finished.template.ldif> は、サービスパッケージとしてディレクトリにインストールする編集済みの ldif ファイルの名前です。

Schema 2 互換モードの ACI の追加

Schema 2 互換モードで LDAP ディレクトリを使用している場合、ACI をディレクトリに手動で追加して、Delegated Administrator によるディレクトリへのプロビジョニングを有効にする必要があります。次の手順に従います。

▼ Schema 2 互換モードの ACI を追加する

手順 **1. OSI** ルートに次の **2** つの **ACI** を追加します。**/opt/SUNWcomm/config** ディレクトリの **usergroup.ldif** ファイル内に次の **2** つの **ACI** が見つかります。

ugldapbasedn をユーザーグループサフィックスに置き換えてください。編集した usergroup.ldif を LDAP ディレクトリに追加します。

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <local.ugldapbasedn>
########################################
dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <ugldapbasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<ugldapbasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read
to org node";
allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

2. 次の **2** つの **ACI** を **DC** ツリールートサフィックスに追加します。
/opt/SUNWcomm/config ディレクトリの **dctree.ldif** ファイル内に次の **2** つの **ACI** が見つかります。

dctreebasedn を DC ツリーのルートサフィックスで、また *ugldapbasedn* をユーザーグループサフィックスで必ず置き換えてください。編集した dctree.ldif を LDAP ディレクトリに追加します。

```
#
# acis to limit Org Admin Role
#
########################################
# dn: <dctreebasedn>
########################################
dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access deny to dc node";
deny (write,add,delete) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)

dn: <dctreebasedn>
changetype: modify
add: aci
aci: (target="ldap:///($dn),<dctreebasedn>")(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to dc
node"; allow (read,search) roledn = "ldap:///cn=Organization Admin
Role,($dn),<ugldapbasedn>";)
```

3. **DC** ツリーのルートサフィックスに次の **ACI** を追加します。これらの **ACI** は **dctree.ldif** ファイルにはありません。

```
dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Proxy user rights"; allow (proxy)
userdn = "ldap:///cn=puser,ou=DSAME Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix"; allow (all) userdn ="ldap:///cn=dsameuser,ou=DSAME
Users,<ugldapbasedn>";)

dn:<dctreebasedn>
changetype:modify
add:aci
aci: (target="ldap:///<dctreebasedn>")(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all) roledn = "ldap:///cn=Top-level Admin
Role,<ugldapbasedn>";)
```

4. **AMConfig.properties** ファイルの **com.iplanet.am.domaincomponent** プロパティーを **DC** ツリーのルートサフィックスに設定します。

   たとえば、< *AM_base_directory*>/lib/AMConfig.properties ファイルの次の行を編集します。

   編集前

   ```
   com.iplanet.am.domaincomponent=o=isp
   ```

   編集後

   ```
   com.iplanet.am.domaincomponent=o=internet
   ```

5. **Access Manager (**以前の **Identity Server)** の互換モードを有効にします。

   Access Manager コンソールの「管理コンソールサービス」ページで、「ドメインコンポーネントツリーの有効」チェックボックスを選択して、有効にします。

6. **inetdomain** オブジェクトクラスを **DC** ツリーのすべてのノード **(dc=com,o=internet** など**)** に追加します。次に例を示します。

   ```
   /var/mps/serverroot/shared/bin 298% ./ldapmodify
   -D "cn=Directory Manager" -w password
   dn: dc=com,o=internet
   changetype: modify
   add: objectclass
   objectclass: inetdomain
   ```

7. **Web** コンテナを再起動します。

第 4 章

Delegated Administrator のカスタマイズ

設定プログラム (`config-commda`) で Delegated Administrator をインストールし設定したあと、個々のニーズに合わせて設定をカスタマイズできます。この章では、Delegated Administrator の特定の機能をカスタマイズする方法の例を示します。

カスタマイズを開始する前に、Delegated Administrator の既存の設定ファイルをバックアップしてください。

また、Delegated Administrator のアップグレード時にも、カスタマイズされた設定データが失われる可能性があります。したがって、Delegated Administrator をアップグレードする前、または Delegated Administrator 設定プログラムを再実行する前に、カスタマイズした設定を保存してください。詳細については、56 ページの「既存の設定の保存」を参照してください。

この章では次の項目について説明します。

サーバー全体のデフォルトを使った優先メールホストの設定

サーバー全体のデフォルトを使用して優先メールホストと優先メールストアを設定する場合は、この項で説明されている手順を実行します。

「優先メールホスト」フィールドをコンソール (特に「新規組織」ウィザードや「組織のプロパティー」画面) から削除する必要がある場合は、次の手順に従います。

- `Security.properties` ファイルを編集します。この手順は、この項で説明します。
- MailHostStorePlugin を使用できるようにします。この手順は次の87 ページの「Delegated Administrator のプラグインの追加」で説明します。

`Security.properties` ファイルを使用すると、すべてのロールまたは個別のロールについて Delegated Administrator コンソールをカスタマイズできます。

`Security.properties` ファイルは *da_base*`/da/WEB-INF/classes/com/sun/comm/da/resources` ディレクトリに格納されています。

コンソールから優先メールホストを削除するには、`Security.properties` ファイルに次に示す行を追加します。

```
# Remove Preferred Mail Host from UI
*.NewOrganizationPage6.PreferredMailHostProperty=INVISIBLE
*.NewOrganizationSummaryPage.PreferredMailHostSummaryProperty=INVISIBLE
*.OrgProperties.MailHostName=INVISIBLE
*.OrgProperties.MailHostNameText=INVISIBLE
*.OrgProperties.MailHostValue=INVISIBLE
```

注意: 個別にカスタマイズする場合にこのファイルに行を追加できますが、既存の行を編集しないでください。既存の行を編集すると、コンソールで例外がスローされる場合があります。

ファイルのプロパティーは次の形式です。*Security Element Name=Permission*

Security Element Name は次の形式です。*Role Name* . *Container View Name* . *Console Element Name*

Security Element は、アクセス権を定義するコンソールの要素とロールを指定します。要素名がわからない場合、ページのソースを表示し、ページに表示される名前と該当するコンソール要素を一致させます。

ページの名前は完全修飾名です。*Container View Name* . *Console Element Name* の形式をとる名前の最後の 2 要素のみをピックアップする必要があります。

Delegated Administrator のロール名に使用できるのは次の名前です。

“ProviderAdminRole” (SPA) このロールの詳細については、付録 A を参照してください。

“OrganizationAdminRole” (OA)

“Top-levelAdminRole” (TLA)

“*” (特定のロールに対してアクセス権がオーバーライドされないかぎり、すべてのロールにアクセス権が適用される)

アクセス権は次の文字列のいずれかとします。

- EDITABLE– セキュリティー要素が編集可能であることを示します。

- NONEDITABLE– セキュリティー要素が読み取り専用であることを示します。
- VISIBLE– セキュリティー要素が表示可能で読み取り専用であることを示します。
- INVISIBLE– セキュリティー要素が非表示であることを示します。

Delegated Administrator のプラグインの追加

次のプラグインをサポートするように Delegated Administrator をカスタマイズできます。

- `MailHostStorePlugin`

  デフォルトでは、このプラグインは無効になっています。ビジネス組織が作成されたときに `preferredmailhost` が指定されていない場合は、例外が発生します。このプラグインが使用可能になっている場合は、対応する属性がないときにフラットファイル (この項の後半で説明) の値が使用されます。

- `MailDomainReportAddressPlugin`

  ドメイン値を使って、任意の DSN アドレスを返します。デフォルトの実装では、文字列 `MAILER-DAEMON@<`*domain* `>` を返します。

- `UidPlugin`

  固有の id 文字列を生成します。デフォルトでは、GUID を呼び出し元に返します。

プラグインを使用可能にする

これらのプラグインを使用可能にする場合は、次のディレクトリにある `commcli servlet resource.properties` ファイルを編集します。

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

デフォルトでは、*da_base* は `/opt/SUNWcomm` です。

プラグインは `resource.properties` ファイル内の次の行で始まる部分にあります。

```
#########################
# Plugin Configuration #
#########################
```

それぞれ「`plugin`」というサフィックスが付きます。現在のリストは次のとおりです。

```
jdapi-mailhoststoreplugin=disabled
```

```
jdapi-mailhoststorepluginclass=sun.comm.cli.server.util.MailHostStorePlugin
jdapi-mailhoststorepluginfile=/tmp/mailhostmailstore
jdapi-maildomainreportaddressplugin=enabled
jdapi-maildomainreportaddresspluginclass=sun.comm.cli.server.
  util.MailDomainReportAddressPlugin
jdapi-uidautogenerationplugin=disabled
jdapi-uidautogenerationpluginclass=sun.comm.cli.server.util.UidPlugin
```

プラグイン形式

各プラグインは最低 2 行で、次の形式をとります。

- `jdapi-<`*name*`>plugin= "enabled" | "disabled"`
-

  `jdapi-<`*name*`>pluginclass=sun.comm.cli.server.util/`
  `<`*java class name*`>`

プラグインを使用可能にするには、"disabled" を " enabled" に変更します。

この項に示したすべてのプラグインには、プラグインクラスが供給されています。これらのクラスは、次のディレクトリに存在します。

da_base`/data/WEB-INF/classes/sun/comm/cli/server/util`

これらのクラスには何もする必要はありません。

MailHostStorePlugin に必須の追加フラットファイル

MailHostStorePlugin には、プラグインの 3 行目に含まれるフラットファイルが必要です。このプラグインはフラットファイル内の値を読み取り、属性値を設定するために使用します。プラグインが使用可能になっている場合に、このファイルが存在していないとエラーが発生します。

-

```
jdapi-mailhoststoreplugin
    o jdapi-mailhoststorepluginin=<full file name>
    o file has one line
    o value is that for :
        o preferredmailhost attribute
        o preferredmailmessagestore attribute
    o form
        o <mailhost>:<mailpartition>
```

LDAP オブジェクト作成時のカスタムオブジェクトクラスの追加

Delegated Administrator では、新しいユーザー、グループ、リソース、または組織の LDAP エントリにカスタムオブジェクトクラスを追加できるように設定できます。この作業を行うには、Access Manager によってディレクトリにインストールされたオブジェクト作成テンプレートのうち該当のものをカスタマイズします。

たとえば、BasicUser 作成テンプレートでは、新規ユーザーの作成時に追加するオブジェクトクラスと属性が決定されます。BasicUser 作成テンプレートは、独自のカスタムオブジェクトクラスを使用して更新できます。更新後は、カスタムオブジェクトクラスが標準のオブジェクトクラスとともに各新規ユーザーに追加されます。

BasicUser テンプレートをカスタマイズする方法を次に示します。同じ手順を BasicGroup、BasicResource、および BasicOrganization の各作成テンプレートのカスタマイズに適用できます。

▼ ユーザー作成プロセスにカスタムオブジェクトクラスを追加する

手順

1. カスタムオブジェクトクラスがディレクトリスキーマに定義されていることを確認します。
2. 次のディレクトリエントリを見つけます。

   ```
   ou=basicuser,ou=creationtemplates,ou=templates,ou=default,
   ou=globalconfig,ou=1.0,ou=dai,ou=services,
   o=$Root_Suffix
   ```

   $Root_Suffix はディレクトリのルートサフィックスです。
3. 次の *attribute:value* をエントリに追加します。

   ```
   sunkeyValue:required=objectClass=$Your_Custom_Objectclass.
   ```

   $Your_Custom_Objectclass はカスタムオブジェクトクラスです。

ユーザーログインのカスタマイズ

Delegated Administrator 設定プログラム (config-commda) を実行すると、Delegated Administrator のログインに使用する値が uid に設定されます。

たとえば、TLA としてログインするとき、TLA の uid が jhon.doe である場合は、jhon.doe で Delegated Administrator にログインします。

Delegated Administrator をカスタマイズして、ユーザーログインに使用する値を追加することができます。たとえば、メールアドレス (mail) を追加できます。

ユーザーログイン値の設定方法

config-commda プログラムは resource.properties ファイルの loginAuth-idAttr プロパティーを使用して、この値を uid に設定します。次に例を示します。

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
```

<$rootSuffix> はディレクトリのルートサフィックスです。

resource.properties ファイル内の次の場所にあります。

da_base/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties

ユーザーログイン値の追加

resource.properties ファイルを編集すると、ユーザーログイン値を追加できます。

たとえば、resource.properties ファイルに次の行を追加すると、メールアドレス (john.doe@sesta.com など) をログインに使用できます。

```
loginAuth-searchBase=<$rootSuffix>
         servicepackage-cosdefbasedn = <$rootSuffix>
          loginAuth-idAttr-1=uid
          loginAuth-idAttr-2=mail
```

<$rootSuffix> はディレクトリのルートサフィックスです。

新しい値を追加するたびに loginAuth-idAttr プロパティーの数値も増やす必要があることに注意してくださいこの例では、2 つ目の値を追加したため、loginAuth-idAttr に -2 を追加しています。

loginAuth-idAttr プロパティーには、複数のインスタンスを追加できます。

```
loginAuth-idAttr-1=uid
  loginAuth-idAttr-2=mail
  |
  loginAuth-idAttr-n=<login-in value>
```

新規ユーザーへのサービスパッケージの割り当てを必須とする

Delegated Administrator のデフォルトでは、サービスパッケージをユーザーに割り当てずに新しいユーザーを作成することができます。

このデフォルト設定を変更して、すべての新規ユーザーに少なくとも 1 つのサービスパッケージを割り当てるようにすることができます。

▼ 新規ユーザーへのサービスパッケージの割り当てを必須とする

手順

1. **daconfig.properties** ファイルをテキストエディタで開きます。

   デフォルトでは、daconfig.properties ファイルは次のディレクトリにあります。

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/
   comm/da/resources/daconfig.properties
   ```

2. **user.atleastOneServicePackage** プロパティーの値を **false** から **true** に変更します。

   デフォルト値は false です。

   次に例を示します。

   ```
   user.atleastOneServicePackage=true
   ```

   この値を true に設定したあと、Delegated Administrator コンソールの「新規ユーザー作成」ウィザードを使用して新しいユーザーを作成するときには、少なくとも 1 つのサービスパッケージを割り当てる必要があります。

新規カレンダタイムゾーンの追加

新しい Calendar Server タイムゾーンを追加して、Delegated Administrator をカスタマイズすることができます。そのあと、Delegated Administrator は新しいタイムゾーンを使用して、組織、ユーザー、グループ、およびリソースをプロビジョニングすることができます。

追加したタイムゾーンは、新規ユーザー作成時のデフォルトタイムゾーンとして設定できます。

▼ Delegated Administrator に新規タイムゾーンを追加する

手順

1. **Calendar Server** で新しいタイムゾーンを追加します。

   この手順を完了するには、`timezones.ics` ファイルおよびその他の Calendar Server ファイルを編集する必要があります。その手順については、『Sun Java System Calendar Server 管理ガイド』の「Calendar Server のタイムゾーンの管理」の章の「新しいタイムゾーンの追加」を参照してください。

2. **`UserCalendarService.xml`**、**`DomainCalendarService.xml`** 、および **`Resources.properties`** の各ファイルをバックアップします。

   デフォルトでは、xml ファイルは次のディレクトリにあります。

   ```
   /opt/SUNWcomm/lib/services
   ```

   デフォルトでは、`Resources.properties` ファイルは次のディレクトリにあります。

   ```
   /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
   comm/da/resources
   ```

   また、Delegated Administrator をアップグレードする前、または Delegated Administrator 設定プログラムを再実行する前に、カスタマイズした設定データを保存してください。

3. **`UserCalendarService.xml`** ファイルと **`DomainCalendarService.xml`** ファイルを編集して、**Delegated Administrator** に新しいタイムゾーンを追加します。

   デフォルトでは、これらの xml ファイルは次のディレクトリにあります。

   ```
   /opt/SUNWcomm/lib/services
   ```

   - `UserCalendarService.xml` ファイルと `DomainCalendarService.xml` ファイルの両方で、次のエントリの見出しを探します。

```
<AttributeSchema name="icstimezone"
                              type="single choice"
                              syntax="string"
                              any="optional|adminDisplay">
                              <ChoiceValues>
```

- <ChoiceValues> のリストに新しいタイムゾーンの値を追加します。

4. **Access Manager** の **amadmin** ユーティリティを実行して、現在のサービスを削除し、更新されたサービスを追加します。

   UserCalendarService.xml ファイルと DomainCalendarService.xml ファイルの両方に対して、次の amadmin コマンドを実行します。

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
```

```
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

注 – また、新しいタイムゾーンをデフォルトにする場合、両方のタスクの実行後にこれらの amadmin コマンドを実行します。次のタスクで、デフォルトのタイムゾーンを変更する方法について説明します。

---

5. **Web** コンテナを再起動して、変更を有効にします。

▼ Delegated Administrator のデフォルトタイムゾーンを変更する

手順 1. **UserCalendarService.xml** と **DomainCalendarService.xml** の各ファイルで次の値を編集します。

```
<DefaultValues>
                <Value>America/Denver</Value>
</DefaultValues>
```

<DefaultValues> は xml ファイルの次のエントリの下にあります。

```
<AttributeSchema name="icstimezone"
```

2. **Access Manager** の **amadmin** ユーティリティを実行して、現在のサービスを削除し、更新されたサービスを追加します。

   UserCalendarService.xml ファイルと DomainCalendarService.xml ファイルの両方に対して、次の amadmin コマンドを実行します。

```
./amadmin -u <admin> -w <password> -r DomainCalendarService
```

```
./amadmin -u <admin> -w <password> -s $PATH/DomainCalendarService.xml
```

3. **Web** コンテナを再起動して、変更を有効にします。

▼ 新規タイムゾーンを Delegated Administrator コンソールに追加する

手順

- **Delegated Administrator** のデータディレクトリにある **`Resources.properties`** ファイルを編集します。

  デフォルトでは、`Resources.properties` ファイルは次のディレクトリにあります。

  ```
  /var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
  comm/da/resources
  ```

  `Resources.properties` を編集するには、`rsrc.Timezone` プロパティーを検索し、新しいタイムゾーンを該当のリストに追加します。

  このファイルの編集後は、新しいタイムゾーンが Delegated Administrator コンソールの該当するリストボックスに表示されます。

第 5 章

コマンド行ユーティリティー

Delegated Administrator コマンド行ユーティリティーを使用すると、管理者はユーザー、グループ、ドメイン、組織に対して異なる通信サービスを管理できます。この章では、ユーザー、グループ、ドメイン、組織の作成、変更、削除、検索などの一括操作の実行に使用するコマンド行ツールについて説明します。

コマンド

次の表にコマンドの一覧を示します。この表は 3 つの列から構成されます。最初の列にはコマンド、2 番目の列にコマンドの説明、3 番目の列にコマンドの実行を許可される管理者のタイプが示されます。

`commadmin` ユーティリティーは、`/opt/SUNWcomm/bin` ディレクトリ内にあります。

表 **5–1** Delegated Administrator のコマンド行インタフェース

コマンド	説明	実行許可*
99 ページの「commadmin admin add」	ユーザーに組織管理者権限を与えます	最上位管理者
100 ページの「commadmin admin remove」	ユーザーの組織管理者権限を破棄します	最上位管理者
102 ページの「commadmin admin search」	組織管理者権限を持つユーザーを検索し表示します	最上位管理者、組織管理者
102 ページの「commadmin domain create」	ドメインを作成します	最上位管理者

表 **5–1** Delegated Administrator のコマンド行インタフェース　(続き)

コマンド	説明	実行許可*
105 ページの「commadmin domain delete」	ドメインを削除します	最上位管理者
107 ページの「commadmin domain modify」	ドメインを変更します	最上位管理者
109 ページの「commadmin domain purge」	ドメインを破棄します	最上位管理者
112 ページの「commadmin domain search」	ドメインを検索します	最上位管理者
113 ページの「commadmin group create」	グループを作成します	最上位管理者、組織管理者、メールリスト所有者
116 ページの「commadmin group delete」	グループを削除します	最上位管理者、組織管理者、メールリスト所有者
117 ページの「commadmin group modify」	グループを変更します	最上位管理者、組織管理者、メールリスト所有者
120 ページの「commadmin group search」	グループを検索します	すべて
122 ページの「commadmin resource create」	リソースを作成します	最上位管理者、組織管理者
127 ページの「commadmin resource modify」	リソースを変更します	最上位管理者、組織管理者
125 ページの「commadmin resource delete」	リソースを削除します	最上位管理者、組織管理者
128 ページの「commadmin resource search」	リソースを検索します	すべて
130 ページの「commadmin user create」	ユーザーを作成します	最上位管理者、組織管理者
133 ページの「commadmin user delete」	ユーザーを削除します	最上位管理者、組織管理者
138 ページの「commadmin user search」	ユーザーを検索します	すべて
135 ページの「commadmin user modify」	ユーザーを変更します	最上位管理者、組織管理者
* Delegated Administrator の今回のリリースでは、サービスプロバイダ管理者による `commadmin` ユーティリティーの使用はサポートされていません。		

実行モード

コマンド行の実行には 3 つのモードがあります。

- ファイルで指定されたオプションによる実行

  `commadmin` *object task* `-i` *inputfile*

  inputfile を分析し、実行します。
- 対話型

  `commadmin` *object task*

  オプションおよび属性の通知について、管理者に照会されます。
- 即時実行またはシェル実行

  `commadmin` *object task* [*options*]

`commadmin` の処理に成功すると、コマンド行に OK メッセージが表示されます。

失敗した場合は、次のメッセージが表示されます。

`FAIL`

<*message*>

<*message*> の部分にはエラーテキストが表示されます。

コマンドファイルの形式

オプションは `-i` オプションを使用してファイル内で指定できます。

ファイル内では、オプション名は空白でオプション値と区切られます。オプション値は空白以外の文字から始まり、行の行末文字まで続きます。オプションの組と組の間は空行で区切ります。

一般的な構文は次のようになります。

```
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
<blank line>
<option name><white space>[option value, if any]
<option name><white space>[option value, if any]
...
<option name><white space>[option value, if any]
```

コマンド行に指定したオプション値は、各オプションのデフォルトになります。または、各オプションにこれらのオプションを指定できます。この場合、コマンド行で指定されたデフォルトがこの値で上書きされます。

次に、commadmin user add コマンドの -i オプションで指定されるファイルの形式と構文の例を示します。

```
l newuser1
F new
L user1
W secret

l newuser2
F new
L user2
W secret

l newuser3
F new
L user3
W secret

<and so forth...>
```

コマンドの説明

この項では、コマンド行ツールの説明を行い、構文と例を示します。

必須 commadmin オプション

次のオプションは必須です。管理者またはユーザーの認証に使用されます。

オプション	説明
-D *userid*	ディレクトリへのバインドに使用されるユーザー ID。
-w *password*	ディレクトリへの userID の認証に使用されるパスワード。 テキストファイル *password*.txt を使用して *password* を指定することもできます。
-n *domain*	管理者が属するドメイン。

Access Manager Host (-x))、Access Manager Port (-p)、およびデフォルトドメイン (-n) の値は、インストール時に指定され、cli-userprefs.properties ファイルに保存されます。

注 – commadmin コマンドの実行時に、-X、-p、および -n オプションを指定しない場合、これらの値には cli-userprefs.properties ファイルの値が使用されます。

commadmin admin add

commadmin admin add コマンドは特定のドメインのユーザーに、組織管理者権限を与えます。このコマンドは、最上位管理者か ISP 管理者のみが実行できます。

構文

commadmin admin add -D *login* -l *login* -n *domain* -w *password* -d *domain* [-h] [-i *inputfile*] [-p *AM port*] [-X *AM host*] [-?] [-s] [-v] [-V]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	最上位管理者のユーザー ID。
-l *login*	組織の管理権限を付与するユーザーのユーザー ID。ユーザーはディレクトリ内に表示され、-d オプションで指定されるドメインに属している必要があります。
-n *domain*	最上位管理者のドメイン。このドメインを指定しない場合、cli-userprefs.properties ファイルに保存されたデフォルトドメインが使用されます。
-w *password*	最上位管理者のパスワード。
-d *domain*	管理権限を付与するドメイン。指定しない場合、-n オプションで指定されるドメインが使用されます。

次のオプションは任意です。

オプション	説明
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。

オプション	説明
-p *AM port*	このオプションは、Access Manager が待機する代替 TCP ポートを指定する場合に使用します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。
-h, -?	コマンド使用構文を印刷します。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。

例

次の構文では、ユーザー ID admin1 を持つユーザーに組織の管理権限が与えられます。

```
commadmin admin add -D chris -n sesta.com -w bolton -l admin1 \
-d florizel.com
```

次の構文では、ユーザー ID admin2 を持つドメイン florizel.com のユーザーに組織の管理権限が与えられます。

```
commadmin add admin -D chris -w bolton -l admin2 -n varrius.com \
-d florizel.com
```

commadmin admin remove

commadmin admin remove コマンドは、既存の組織管理者から組織管理者権限を削除します。このコマンドを実行できるのは、最上位管理者のみです。

複数のユーザーから組織管理者の権限を削除するには、-i オプションを使用します。

構文

commadmin admin remove -D *login* -l *login* -n *domain* -w *password* -d *domain name* [-h] [-?] [-i *inputfile*] [-p *AM port*] [-X *AM host*] [-s] [-v] [-V]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	最上位管理者のユーザー ID。
-l *login*	管理者権限の破棄が必要なユーザーのユーザー ID。
-n *domain*	最上位管理者のドメイン。
-w *password*	最上位管理者のパスワード。
-d *domain name*	管理者権限を破棄するドメイン。-d を指定しない場合、-n で指定されるドメインが使用されます。

次のオプションは任意です。

オプション	説明
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-p *AM port*	このオプションは、Access Manager が待機する代替 TCP ポートを指定する場合に使用します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。

例

次のコマンドは、ユーザー ID admin5 を持つ管理者から組織管理者権限を削除します。

```
commadmin admin remove -D chris -n sesta.com -w bolton -l admin5 -d test.com
```

commadmin admin search

commadmin admin search コマンドはドメインの特定の、またはすべての組織管理者を検索し、表示します。

構文

commadmin admin search -D *login* -n *domain* -w *password* [-l *login*] [-d *domain*]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-n *domain*	-D オプションで指定されるユーザーのドメイン。
-w *password*	-D オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
-l *login*	検索する組織管理者のユーザー ID。-l が指定されていない場合、またはワイルドカード演算子 (-l* または -l '*') を使用して -l が指定されている場合、ドメインのすべての組織管理者が表示されます。
-d *domain*	指定されたドメインの組織管理者権限を持つユーザーを検索します。-d を指定しない場合、-n で指定されるドメインが使用されます。

例

test.com ドメインのすべての組織管理者を検索するには、次のコマンドを実行します。

```
commadmin admin search -D chris -n sesta.com -w bolton -d test.com
```

commadmin domain create

commadmin domain create コマンドは Access Manager でドメインを 1 つ作成します。複数のドメインを作成するには、-i オプションを使用します。

構文

```
commadmin domain create -D login -d domain name -n domain -w password
[-A [+] attributename:value] [-h] [-?] [-i inputfile] [-o organization RDN] [-p AM port]
[-s] [-v] [-V] [-X AM host] [-S mail -H preferred mailhost]
[-S cal [-B backend calendar data server] [-C searchable domains] [-g access control string]
[-P propertyname[:value]] [-R right[:value]] [-T calendar time zone string]]
```

オプション

次のオプションは必須です。

オプション	説明
-D *login*	最上位管理者のユーザー ID。
-d *domain name*	作成されるドメインの DNS ドメイン名。
-n *domain*	最上位管理者のドメイン。
-w *password*	最上位管理者のパスワード。

次のオプションは任意です。

オプション	説明
-A [+]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、指定した *value* により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。 アクション値 (+) を指定しない場合、デフォルトアクションでは既存の値が追加されます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-o *organization RDN*	ドメインの組織の RDN を指定します。たとえば、o=varrius.florizel.com です。 このオプションが指定されていない場合、組織は「o=ドメイン名」の o=osiSuffix を持つ osi suffix の下に作成されます。

オプション	説明
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。
-S *service*	ドメインに追加されるサービスを指定します。 *service* には単一のサービスまたは複数のサービスの値を指定できます。*service* に使用できる値は mail および cal です。これらの値は大文字と小文字を区別しません。 -S mail オプションを指定する場合、-H オプションを指定する必要があります。 コンマ区切りリストとして一覧表示できます。 例 -S mail,cal ドメインは、特定のサービス定義の値に従って述べられるサービスを Identity Server の設定ファイル内に示して作成します。
次のオプションは、-S mail オプションを指定した場合にのみ使用できます。	
-H *preferred mailhost*	ドメインの優先メールホスト。このホストは mailhost.sesta.com など、完全修飾ホスト名でなければいけません。 このオプションは、-S mail オプションが指定されている場合は必須です。
次のオプションは、-S cal オプションを指定した場合にのみ使用できます。	
-B *backend calendar data server*	ドメインのユーザーまたはリソースに割り当てられるデフォルトバックエンドホストを指定します。

オプション	説明
-C *searchable domains*	カレンダまたはユーザーを検索する場合、検索されるドメインを指定します。
-g *access control string*	新しく作成されたユーザーカレンダの ACL (アクセス制御リスト) を指定します。
-P *propertyname*[: *value*]	多値属性またはビット指向属性の値を設定します。属性、属性の説明、および属性値については、165 ページの「属性値」の表を参照してください。
-R *right*[:*value*]	カレンダドメイン属性 icsAllowRights を設定します。この属性はビットマップ値を保持します。属性の一覧、属性値、および属性の説明については、165 ページの「属性値」を参照してください。
-T *calendar time zone string*	ファイルのインポート時に使用されるタイムゾーン ID を指定します。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。

例

メールサービスとカレンダサービスで新しいドメインを作成するには、次のように入力します。

```
commadmin domain create -D chris -d florizel.com -n sesta.com -w bolton \
-S mail,cal -H mailhost.sesta.com
```

commadmin domain delete

commadmin domain delete コマンドは、サーバーから削除されたものとして、単一のホストドメインをマークします。複数のホストドメインを削除済みとしてマークするには、-i オプションを使用します。

109 ページの「commadmin domain purge」 コマンドはドメインを永続的に削除します。

カレンダサービスやメールサービスなどのサービスの組織管理者による使用を無効にするには、-S オプションを使用します。S は大文字です。

構文

commadmin domain delete -D *login* -d *domain name* -n *domain* -w *password* [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-S *service*] [-v] [-V] [-X *AM host*]

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	最上位管理者のユーザー ID。
`-d` *domain name*	削除される DNS ドメイン名。`-d` を指定しない場合、`-n` で指定されるドメインが使用されます。
`-n` *domain*	最上位管理者のドメイン。
`-w` *password*	最上位管理者のパスワード。

次のオプションは任意です。

オプション	説明
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-S` *service*	指定されたサービスのステータス属性の値を「deleted」に変更します。 複数のサービスはコンマで区切ります。*service* に使用できる値は `mail` および `cal` です。これらの値は大文字と小文字を区別しません。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

既存のドメインを削除するには、次のコマンドを実行します。

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com
```

florizel.com ドメインからメールサービスのみを削除するには、次のコマンドを実行します。

```
commadmin domain delete -D chris -w bolton -d florizel.com -n sesta.com \
-S mail
```

commadmin domain modify

commadmin domain modify コマンドは、単一ドメインのディレクトリエントリの属性を変更します。複数のドメインを変更するには、-i オプションを使用します。

構文

commadmin domain modify -D *login* -d *domain* -n *domain* -w *password*
[-A [+|-]*attributename*:*value*] [-h] [?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V]
[-X *AM host*] [-S mail -H *preferred mailhost*] [-S cal [-g *access string*]
[-C *cross domain search domains*] [-B *backend calendar data server*]
[-P [*action*]*propertyname*[: *value*]] [-R *propertyname*[:*value*]] [-T *calendar time zone string*]]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	最上位管理者のユーザー ID。
-d *domain*	変更する DNS ドメイン名。-d を指定しない場合、-n で指定されるドメインが使用されます。
-n *domain*	最上位管理者のドメイン。
-w *password*	最上位管理者のパスワード。

次のオプションは任意です。

オプション	説明
`-A` [`+` | `-`]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、値により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。「-」は値の削除を示します。 コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けます。入力ファイル内でオプションを指定する場合、「-」記号の前に円記号を 1 つ付けます。 アクション値 (+ または -) を指定しない場合、デフォルトアクションでは既存の値が置き換わります。
`-h, -?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。
`-S` *service*	変更中に、指定されたサービスをドメインに追加します。 *service* に使用できる値は `mail` および `cal` です。これらの値は大文字と小文字を区別しません。 `-S` オプションで一覧表示されるサービスは、コンマで区切られます。 `-S mail` を指定する場合、`-H` オプションを指定する必要があります。

オプション	説明
サービスを追加する場合、次のオプションは、`-S mail` オプションを指定した場合にのみ使用できます。	
`-H` *preferred mailhost*	ドメインの優先メールホスト。 このオプションは、`-S mail` オプションが指定されている場合は必須です。
サービスを追加する場合、次のオプションは、`-S cal` オプションを指定した場合にのみ使用できます。	
`-B` *backend calendar data server*	ドメインのユーザーまたはリソースに割り当てられるデフォルトバックエンドホスト。
`-C` *cross domain search domains*	カレンダまたはユーザーを検索する場合、検索されるドメインを指定します。
`-g` *access string*	新しく作成されたユーザーカレンダの ACL (アクセス制御リスト) を指定します。
`-P` [*action*]*propertyname* [:*value*]	多値属性またはビット指向属性の値を設定します。*propertyname* の説明と値については、165 ページの「属性値」の表を参照してください。
`-T` *calendar time zone string*	ファイルのインポート時に使用されるタイムゾーン ID。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。
`-R` *propertyname*[: *value*]	カレンダドメイン属性 `icsAllowRights` を設定します。この属性はビットマップ値を保持します。属性の一覧、属性値、および属性の説明については、165 ページの「属性値」を参照してください。

例

既存のドメインを変更するには、次のコマンドを実行します。

```
commadmin domain modify -D chris -w bolton -n sesta.com -d varrius.com \
-A preferredmailhost:test.siroe.com
```

commadmin domain purge

`commadmin domain purge` コマンドは削除対象としてマークされたすべてのエントリまたはエントリのサービスを、永続的に削除します。これには、ドメイン、ユーザー、グループ、リソースが含まれます。

定期的な保守作業の一環として、commadmin domain purge コマンドを使用して、指定された猶予期間を過ぎても「deleted」になっているすべてのエントリを削除します。

コマンドを手動で呼び出すことにより、いつでも破棄を実行できます。

コマンドを呼び出した場合、ディレクトリが検索され、指定された猶予期間を過ぎても削除にマークされているドメインのリストが作成されます。猶予期間のデフォルト値は 5 日間です。

-d* オプションを指定した場合、「deleted」とマークされたユーザーとドメインがすべてのドメインで検索されます。「deleted」とマークされたユーザーはそのドメインから破棄されますが、ドメインは「deleted」とマークされないかぎり破棄されません。ドメインに「deleted」とマークされた場合、そのドメイン内のすべてのユーザーと一緒にドメインが破棄されます。

サービスに「deleted」のマークが付いたあと、メールボックスやカレンダなどのリソースを削除するユーティリティーを実行してから、ディレクトリからサービスを破棄してください。メールサービスの場合、このプログラムは msuserpurge と呼ばれています。msuserpurge ユーティリティーについての詳細は、『Sun Java System Messaging Server Administration Reference』を参照してください。カレンダサービスの場合、このプログラムは csclean です。csclean ユーティリティーについての詳細は、『Sun Java System Calendar Server 管理ガイド』を参照してください。

注 – commadmin domain purge コマンドは必ず最上位管理者が実行します。

構文

commadmin domain purge -D *login* -n *domain* -w *password* -d *domain* [-g *grace*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-S *service*] [-v] [-V] [-X *AM host*]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	最上位管理者のユーザー ID。
-n *domain*	最上位管理者のドメイン。
-w *password*	最上位管理者のパスワード。
-d *domain*	指定されたドメインを破棄します。* 演算子 (-d*) を使用してパターン検索を実行できます。

次のオプションは任意です。

オプション	説明
-g *grace*	ドメインが破棄されるまでの猶予期間 (日数)。削除がマークされ、*grace* の日数が経過する前のドメインは、破棄されません。0 は即時破棄を意味します。デフォルト値は 5 日間です。デフォルト値を永続的に変更することはできません。猶予期間は、commadmin domain purge コマンドで -g *grace* オプションを使用してのみ変更できます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-S *service*	サービスに関連したオブジェクトクラスと属性を、ドメインから削除します。ドメインにユーザーとリソースが含まれている場合、これらのユーザーとリソースに関するサービス固有のデータが、ディレクトリから削除されます。 サービスのリストはコンマ (,) 区切り文字で区切られます。 *service* に使用できる値は mail および cal です。これらの値は大文字と小文字を区別しません。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

次の例では、siroe.com ドメインが破棄され、そのドメイン内のすべてのエントリも削除されます。

```
commadmin domain purge -D chris -d siroe.com -n sesta.com -w bolton
```

commadmin domain search

`commadmin domain search` コマンドは、単一ドメインに関連したすべてのディレクトリのプロパティーを取得します。複数のドメインのディレクトリプロパティーをすべて取得する場合は、`-i` オプションを使用します。このコマンドで `-s` を指定した場合、指定されたサービスがアクティブになっているドメインのみが表示されます。

構文

`commadmin domain search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-S` *service*`] [-t` *Search Template*`] [-v] [-V] [-X` *AM host*`]`

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
`-d` *domain*	このドメインを検索します。`-d` が指定されていない、または `-d*` が指定されている場合、すべてのドメインが表示されます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。

オプション	説明
`-S` *service*	アクティブなドメインで検索するサービスを指定します。 *service* には単一のサービスまたは複数のサービスの値を指定できます。*service* に使用できる値は `mail` および `cal` です。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 `-S mail,cal`
`-t` *Search template*	デフォルトの検索テンプレートの代わりに使用する検索テンプレートの名前を指定します。検索のあと、アクティブなドメインのみが表示されます。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

commadmin group create

`commadmin group create` コマンドは Access Manager にグループを 1 つ追加します。複数のグループを作成するには、`-i` オプションを使用します。

メンバーを含まないグループを作成する場合は、デフォルトではスタティックグループになります。

注 – グループにはスタティックメンバーもダイナミックメンバーも含めることができません。

電子メール配布リストもグループのタイプの 1 つです。メッセージがグループアドレスに送信されると、Access Manager はグループ内のすべてのメンバーにメッセージを送信します。

構文

`commadmin group create -D` *login* `-G` *groupname* `-n` *domain* `-w` *password*
`[-A [+]`*attributename*`:`*value*`] [-d` *domain*`] [-f` *ldap-filter*`] [-h] [-?] [-i` *inputfile*`]`
`[-m` *internal-member*`] [-p` *AM port*`] [-s] [-v] [-V] [-X` *AM host*`] [-S` *service* `[-H` *mailhost*`]`
`[-E` *email*`] [-M` *external-member*`] [-o` *owner*`] [-rs` *moderator*`]]`

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-G` *groupname*	グループの名前 (例: `mktg-list`)。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
`-A` [+]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、*value* により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。
`-d` *domain*	グループの完全修飾ドメイン名 (例: `varrius.com`)。デフォルトはローカルドメインです。`-d` を指定しない場合、`-n` で指定されるドメインが使用されます。
`-f` *ldap-filter*	ダイナミックグループを作成します。 属性または属性の組み合わせを指定して、LDAP フィルタを設定します。 `-f` コマンドを複数指定すると、グループの複数のメンバーに対して多くの LDAP フィルタを定義できます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-m` *internal -member*	このグループに追加される内部メンバーのユーザーID。複数のメンバーを追加するには、複数の `-m` オプションを使用します。 このオプションはスタティックグループの作成に使用します。

オプション	説明
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-S *service*	グループに追加するサービスを指定します。 *service* には単一のサービスまたは複数のサービスの値を指定できます。service の値には mail と cal が使用できます。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 `-S mail,cal`
次のオプションは、-S mail オプションを指定した場合にのみ使用できます。	
-H *mailhost*	このグループが応答するメールホスト (例: mailhost.varrius.com)。デフォルトはローカルメールホストです。
-E *email*	グループの電子メールアドレス。
-M *external-member*	このグループに追加される外部メンバーのユーザーID。複数のメンバーを追加するには、複数の -M オプションを使用します。
-o *owner*	グループの所有者の電子メールアドレス。所有者は配布リストを担当する個人ユーザーです。 所有者は配布リストのメンバーを追加または削除できます。
-r *moderator*	モデレータの電子メールアドレス。

例

ドメイン sesta.com のグループ testgroup を作成するには、次のコマンドを実行します。

```
commadmin group create -D chris -n sesta.com -w bolton -G testgroup \
-d sesta.com -m lorca@sesta.com -S mail -M achiko@varrius.com
```

commadmin group delete

commadmin group delete コマンドは単一グループに「deleted」をマークします。複数のグループに「deleted」をマークするには、-i オプションを使用します。

グループによる Calendar Server や Messaging Server などのサービスの利用を無効にする場合は、-S オプションを使用します。S は大文字です。

注 – グループを永続的に削除するためには、 次のコマンドを実行する必要があります。109 ページの「commadmin domain purge」

構文

```
commadmin group delete -D login -G groupname -n domain -w password [-d domain] [-h]
[-?] [-i inputfile] [-p AM port] [-s] [-S service] [-v] [-V] [-X AM host]
```

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-G *groupname*	「deleted」をマークするグループの名前。たとえば、mktg-list。
-n *domain*	-D オプションで指定されるユーザーのドメイン。
-w *password*	-D オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
-d *domain*	グループのドメイン。-d を指定しない場合、-n オプションで指定されるドメインが使用されます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-S *service*	指定されたサービスのステータス属性の値を「deleted」に変更します。 -S オプションで一覧表示されるサービスは、コンマで区切られます。*service* に使用できる値は mail および cal です。これらの値は大文字と小文字を区別しません。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

次の例では、testgroup@varrius.com のグループに「deleted」がマークされます。

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com
```

次の例では、testgroup@varrius.com のメールサービスに「deleted」がマークされます。

```
commadmin group delete -D chris -n sesta.com -w bolton -G testgroup \
-d varrius.com -S mail
```

commadmin group modify

commadmin group modify コマンドは、Access Manager にすでに存在する単一のグループの属性を変更します。複数のグループの属性を変更するには、-i オプションを使用します。

メーリングリストも 1 種のグループです。メッセージがグループアドレスに送信されると、Access Manager はグループ内のすべてのメンバーにメッセージを送信します。

構文

```
commadmin group modify -D login -G groupname -n domain -w password
[-A [+|-]attributename:value] [-d domain] [-f [action]ldap-filter] [-h] [-?] [-i inputfile]
[-m [+|-]internal-member] [-p AM port] [-s] [-v] [-V] [-X AM host]
[-S mail [-o owner] [-E email] [-H mailhost] [-M external-member] [-r moderator]]
```

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-G *groupname*	変更するグループの名前。たとえば、mktg-list。
-n *domain*	-D オプションで指定されるユーザーのドメイン。
-w *password*	-D オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
-A [+	-]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、値により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。「-」は値の削除を示します。コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けるか、引用符で囲みます。入力ファイル内でオプションを指定する場合、「-」記号の前に円記号を 1 つ付けます。
-d *domain*	グループのドメイン。-d を指定しない場合、-n オプションで指定されるドメインが使用されます。

オプション	説明
- f [*action*] *ldap-filter*	ldap フィルタをグループに追加するか、グループから削除するか指定します。 *ldap-filter* の前の「+」は、既存のフィルタに追加されることを示します。「-」は既存のフィルタの削除を示します。すべてのフィルタを削除する場合は、-f-* を入力します。コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けるか、引用符で囲みます。 *action* を指定しない場合、デフォルトでは、まだ存在していなければ、このフィルタが追加されます。それ以外の場合、エラーメッセージが表示されます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-m [*action*] *internal -member*	内部メンバーを追加するか削除するかを指定します。 internal-*member* の値は電子メールアドレスかユーザー ID です。 *action* の値 + は内部メンバーの既存のリストにメンバーを追加します。 - は内部メンバーの既存のリストからメンバーを削除します。コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けるか、引用符で囲みます。 -m-* はすべての内部メンバーを削除します。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-x *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

オプション	説明
-S mail	メールサービスがすでに存在するかどうかを検証したあと、変更する間にグループにメールサービスを追加します。サービスが存在する場合、エラーメッセージが表示されます。 -S の値には、 mail のみ使用できます。
次のオプションは、-S mail オプションを指定した場合にのみ使用できます。	
-o *owner*	グループの所有者の電子メールアドレス。所有者は配布リストを担当する個人ユーザーです。 所有者は配布リストのメンバーを追加または削除できます。
-E *email*	グループの電子メールアドレス。
-H *mailhost*	グループのメールホスト。デフォルトはローカルメールホストです。
-M *external -member*	外部メンバーを追加します。 *external-member* の値はユーザーのメールアドレスです。
-r *moderator*	モデレータのユーザー ID。モデレータが別のドメインに存在する場合、電子メールアドレスを入力します。 このオプションには必ず -S mail オプションを指定します。

例

ドメイン varrius.com 内のグループ testgroup から内部メンバー (jsmith) を削除するには、次のコマンドを実行します。

```
commadmin group modify -D chris -d varrius.com -G testgroup -n sesta.com \
-w bolton -m \\-jsmith
```

commadmin group search

commadmin group search コマンドは、単一グループに関連したすべてのディレクトリのプロパティーを取得します。複数のグループのディレクトリプロパティーをすべて取得する場合は、-i オプションを使用します。

構文

commadmin group search -D *login* -n *domain* -w *password* [-d *domain*] [-E *string*] [-G *string*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-S *service*] [-t *search template*] [-v] [-V] [-X *AM host*]

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
`-d` *domain*	検索するグループのドメイン。`-d` を指定しない場合、すべてのドメインが検索されます。
`-E` *string*	グループの電子メールアドレス。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-G` *string*	検索するグループの名前。たとえば、`mktg-list`。`-G` を指定しない場合、`-d` で指定されたドメインのすべてのグループが表示されます。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	IS サーバーが待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-S` *service*	検索するサービスを指定します。 *service* に使用できる値は `mail` のみです。この値は大文字と小文字を区別しません。 例 `-S mail` サービスが実行中のグループのみが表示されます。

オプション	説明
`-t` *Search Template*	デフォルトの検索テンプレートの代わりに使用する検索テンプレートの名前を指定します。これはディレクトリ内で、検索用フィルタを定義するエントリです。アクティブなグループのみ検索されます。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

`siroe.com` ドメイン内のグループ `developers` を検索するには、次のコマンドを実行します。

```
commadmin group search -D chris -n sesta.com -w password -G developers \
-d siroe.com
```

commadmin resource create

`commadmin resource create` コマンドは、リソースのディレクトリエントリを作成します。

リソースの作成手順については、124 ページの「リソースの作成」を参照してください。

構文

`commadmin resource create -D` *login* `-n` *domain* `-w` *password* `-u` *identifier* `-N` *name* `-o` *owner* `[-c` *calendar identifier*`] [-A [+]` *attributename*`:`*value*`] [-C` *DWPHost*`] [-d` *domainname* `] [-h] [-?] [-i` *inputfile*`] [-p` *AM port*`] [-s] [-T` *time zone*`] [-v] [-V] [-X` *AM host*`]`

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。
`-u` *identifier*	リソースの固有の識別子。 この *identifier* の値は、ドメインの名前空間内、またはカレンダがカレンダモードで管理するすべてのユーザーおよびリソース内で固有でなければいけません。
`-N` *name*	カレンダ GUI でリソースの表示に使用するわかりやすい名前。
`-o` *owner*	リソースの所有者。このユーザー ID は、リソースが作成されたドメイン内に存在する必要があります。
`-c` *calendar identifier*	このリソースのカレンダの識別子。 識別子の値は、Calendar Server で管理されるすべてのカレンダ間で固有でなければいけません。

次のオプションは任意です。

オプション	説明
`-A` [+] *attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、*value* により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。
`-C` *DWPHost*	このユーザーのカレンダをホスティングするバックエンドカレンダサーバーの DNS 名。 バックエンドカレンダサーバーの DNS 名を指定しない場合、サーバーの ics.conf ファイル内に保存されている値がデフォルト値として使用されます。
`-d` *domain name*	リソースのドメイン。`-d` を指定しない場合、`-n` で指定されるドメインが使用されます。
`-h`, `-?`	コマンド使用構文を印刷します。

オプション	説明
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-T` *time zone*	カレンダのユーザーインタフェースでリソースのカレンダを表示するのに使用するタイムゾーン。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

ドメイン `varrius.com` 内のカレンダ `cal.siroe.com` に、`peter` という名前のリソースを作成するには、次のコマンドを実行します。

```
commadmin resource create -D chris -n sesta.com -w bolton -o ownerid \
-d varrius.com -u id -c calid -N peter -C cal.siroe.com
```

リソースの作成

リソースは 2 つのデータ記述から構成されます。Calendar Server データベースのディレクトリエントリとカレンダです。ディレクトリエントリは、リソースに関連したカレンダの名前を値とする属性 `icsCalendar` を持ちます。

2 つのデータ記述から構成されるリソースは、次の方法のいずれかを使用して作成します。

- `csresource` ユーティリティーを単独で使用します。`csresource` ユーティリティーはディレクトリエントリとカレンダを作成します。

  ただし、`csresource` を使用してディレクトリエントリとカレンダの両方を作成することは、ディレクトリが Schema 1 環境であり、Access Manager を使用していない場合のみ推奨されます。

- commadmin resource create を使用してディレクトリエントリを作成し、csresource ユーティリティーを使用してカレンダを作成します。次に例を示します。

  次のように、commadmin resource create を使用してディレクトリエントリを作成します。

  ```
  commadmin resource create -D amadmin -w ampassword -n blink.sesta.com
   -X blink -p 5555 -d varrius.com -o test1 -u resourceOne
   -N firstResource -c resourceOneCalendar
  ```

  ディレクトリエントリは次のようになります。

  ```
  dn: uid=resourceONE,ou=People,o=varrius,o=domainroot
  uid: resrouceONE
  objectClass: icsCalendarResource
  objectClass: top
  cn: firstResource
  icsStatus: active
  icsCalendar: test1@varrius.com:resourceOne
  ```

  csresource を使用してカレンダを作成します。

注: csresource で create コマンドを呼び出すときにリソース名として入力する値は、commadmin resource create の -u オプションに使用する値と同じにする必要があります。

これで任意のユーザーとしてログインし、リソースをイベントに加えることができるようになります。

csresource ユーティリティーの詳細については、『Sun Java System Calendar Server 管理ガイド』の「Calendar Server のコマンド行ユーティリティーのリファレンス」を参照してください。

commadmin resource delete

commadmin resource delete コマンドはリソースに「deleted」をマークします。

注 – リソースを永続的に削除するには、109 ページの「commadmin domain purge」を実行します。

構文

commadmin resource delete -D *login* -u *identifier* -n *domain* -w *password* [-d *domainname*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*]

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。
`-u` *identifier*	リソースの固有の識別子。

次のオプションは任意です。

オプション	説明
`-d` *domainname*	リソースのドメイン。`-d` を指定しない場合、`-n` で指定されるドメインが使用されます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

リソースに「deleted」をマークするには、次のコマンドを実行します。

```
commadmin resource delete -D chris -n sesta.com -w bolton -u bill023
```

commadmin resource modify

`commadmin resource modify` コマンドはリソースを変更します。

構文

```
commadmin resource modify -D login -n domain -w password -u identifier
[-A [+|-]attributename:value] [-d domainname ] [-h] [-?] [-i inputfile] [-N name]
[-p AM port] [-s] [-T time zone] [-v] [-V] [-X sAM host]
```

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。
`-u` *identifier*	リソースの固有の識別子。

次のオプションは任意です。

オプション	説明
`-A` [+	-]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、値により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。「-」は値の削除を示します。 コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けます。入力ファイル内でオプションを指定する場合、「-」記号の前に円記号を 1 つ付けます。
`-d` *domainname*	リソースのドメイン。`-d` を指定しない場合、`-n` で指定されるドメインが使用されます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。

オプション	説明
`-N` *name*	カレンダユーザーインタフェースでリソースの表示に使用するコマンド名。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-T` *time zone*	リソースのカレンダをカレンダ GUI に表示する場合に使用するタイムゾーン。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

新しい共通の名前 `bjones` で、固有の識別子 `bill023` を持つリソースを変更するには、次のコマンドを実行します。

```
commadmin resource modify -D chris -n sesta.com -w bolton -d test.com \
-u bill023 -N bjones
```

commadmin resource search

`commadmin resource search` コマンドはリソースを検索します。

構文

`commadmin resource search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-h] [-?] [-i` *inputfile*`] [-N` *string*`] [-p` *AM port*`] [-s] [-t` *Search Template*`] [-u` *string*`] [-V] [-v] [-X` *AM host*`]`

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
`-d` *domain*	リソースのドメイン。検索は指定されたドメインでのみ実行されます。`-d` が指定されていない場合、または `-d*` が指定されている場合、すべてのドメインが検索されます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-N` *string*	リソースの共通名を入力します。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-p` *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-t` *Search Template*	デフォルトの検索テンプレートの代わりに使用する検索テンプレートの名前を指定します。これはディレクトリ内で、検索用フィルタを定義するエントリです。アクティブなリソースのみ検索されます。
`-u` *string*	指定するリソース識別子は、ドメインの名前空間に対して、またはカレンダが管理するすべてのユーザーおよびリソースに対して固有でなければいけません。 文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。 識別子が指定されない場合、または `-l*` が指定されている場合、検索の間にすべてのリソースが表示されます。
`-v`	デバッグ出力を有効にします。

オプション	説明
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

ドメイン sesta.com でリソース arabella を検索するには、次のコマンドを実行します。

```
commadmin resource search -D serviceadmin -w serviceadmin -n sesta.com \s
-d sesta.com -u arabella
```

commadmin user create

commadmin user create コマンドは Access Manager システムでユーザーを 1 つ作成します。複数のユーザーを作成するには、-i オプションを使用します。

構文

commadmin user create -D *login* -F *firstname* -n *domain* -L *lastname* -l *userid* -w *password* -W *password* [-A [+] *attributename*:*value*] [-d *domain*] [-I *initial*] [-h] [-?] [-i *inputfile*] [-p *AM port*] [-s] [-v] [-V] [-X *AM host*] [-S mail [-E *email*] [-H *mailhost*]] [-S cal [-B *DWPHost*] [-E *email*] [-k *calid_type*] [-J *First Day of Week*] [-T *time zone*]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-F *firstname*	ユーザーのファーストネーム。空白が入らない単一の語です。
-n *domain*	-D オプションで指定されるユーザーのドメイン。
-l *userid*	ユーザーのログイン名。
-w *password*	-D オプションで指定されるユーザーのパスワード。

オプション	説明
-W *password*	作成されるユーザーのパスワード。 テキストファイル *password*.txt を使用して *password* を指定することもできます。
-L *lastname*	ユーザーの名字。

次のオプションは任意です。

オプション	説明
-A [+]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、*value* により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。
-d *domain*	ユーザーのドメイン。-d を指定しない場合、-n で指定されるドメインが使用されます。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-I *initial*	ユーザーのミドルイニシャル。
-h, -?	コマンド使用構文を印刷します。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

オプション	説明
-S *service*	作成の間に、指定されたサービスをユーザーに追加します。*service* には単一のサービスまたは複数のサービスの値を指定できます。*service* に使用できる値は mail および cal です。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 -S mail,cal
次のオプションは、-S mail オプションを指定した場合にのみ使用できます。	
-E *email*	ユーザーの電子メールアドレス。
-H *mailhost*	ユーザーのメールホスト。
次のオプションは、-S cal オプションを指定した場合にのみ使用できます。	
-B *DWPHost*	このユーザーのカレンダをホスティングするバックエンドカレンダの DNS 名。
-E *email*	カレンダユーザーの電子メールアドレス。
-J *First Day of Week*	カレンダサーバーのユーザーインタフェースにカレンダが表示されるときに示される最初の曜日。有効な値は 0 〜 6 (0 は日曜、1 は月曜...) です。
-k *calid_type*	作成されるカレンダ ID のタイプを指定します。使用できる値は legacy と hosted です。-k legacy を指定した場合、そのカレンダの ID のみが使用されます (例: jsmith)。-k hosted を指定した場合、そのカレンダの ID とドメインが使用されます (例: jsmith@sesta.com)。 -k オプションを指定しない場合は、デフォルトであるカレンダ ID とドメイン (hosted) が使用されます。 -k オプションを指定しない場合に作成されるカレンダ ID タイプの値を設定できます。これは、resource.properties ファイルに次のパラメータを追加して行います。 switch-caltype=*value* *value* は 「hosted」または「legacy」です。 resource.properties ファイルは、次のディレクトリにあります。 *da_base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties

オプション	説明
`-T` *time zone*	ユーザーのカレンダが表示されるタイムゾーン。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。

例

新しいユーザー `smith` を作成するには、次のコマンドを入力します。

```
commadmin user create -D chris -n sesta.com -w secret -F smith -l john \
-L major -W secret -S mail -H mailhost.siroe.com
```

commadmin user delete

`commadmin user delete` コマンドは単一ユーザーに「deleted」をマークします。複数のユーザーに「deleted」をマークするには、`-i` オプションを使用します。

削除取り消しユーティリティーはありません。ただし、`ldapmodify` コマンドを使用すると、破棄の猶予期間が経過して、ユーザーエントリに対して破棄の実行が設定されるまでに、ユーザーエントリのステータス属性を `active` に変更することができます。

▼ ユーザーを削除する

手順

1. **`commadmin user delete`** コマンドを実行して、ユーザーに「**deleted**」をマークします。
2. ユーザーからリソースを削除します。
   リソースとしては、メールボックスやカレンダなどがあります。

   メールサービスの場合、このプログラムは `msuserpurge` と呼ばれています。`msuserpurge` ユーティリティーについての詳細は、『Sun Java System Messaging Server Administration Reference』を参照してください。

   カレンダサービスの場合、このプログラムは `csclean` です。`csclean` ユーティリティーについての詳細は、『Sun Java System Calendar Server 管理ガイド』を参照してください。
3. 次のコマンドを呼び出し、ユーザーを永続的に削除します。109 ページの「**commadmin domain purge**」。

構文

```
commadmin user delete -D login -n domain -l login name -w password [-d domain] [-h]
```

[-?] [-i *inputfile*] [-p *AM port*] [-s] [-S *service*] [-v] [-V] [-X *AM host*]

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-n *domain*	-D オプションで指定されるユーザーのドメイン。
-w *password*	-D オプションで指定されるユーザーのパスワード。
-l *userid*	削除するユーザーのユーザー ID。

次のオプションは任意です。

オプション	説明
-d *domain*	ユーザーのドメイン。-d を指定しない場合、-n で指定されるドメインが使用されます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-S *service*	ユーザーから削除するサービスを指定します。ユーザーは引き続きアクティブな状態ですが、指定されたサービスのみが停止します。-S を指定しない場合、そのユーザーが削除されます。 *service* には単一のサービスまたは複数のサービスの値を指定できます。*service* の値には mail と cal が使用できます。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 -S mail,cal
-v	デバッグ出力を有効にします。

オプション	説明
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

既存のユーザーに「deleted」をマークするには、次のコマンドを実行します。

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith
```

メールサービスをユーザー smith だけから削除するには、次のコマンドを実行します。

```
commadmin user delete -D chris -n sesta.com -w bolton -l smith -S mail
```

commadmin user modify

commadmin user modify コマンドは、単一ユーザーのディレクトリエントリの属性を変更します。複数のユーザーを変更するには、-i オプションを使用します。

構文

```
commadmin user modify -D login -n domain -l userid -w password
[-A [+|-]attributename:value] [-d domain] [-h] [-?] [-i inputfile] [-p AM port] [-s]
[-v] [-V] [-X AM host] [-S mail -H mailhost [-E email]] [-S cal [-B DWPHost]
[-E email] [-k calid_type] [-J First Day of Week] [-T time zone]]
```

オプション

次のオプションは必須です。

オプション	説明
-D *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
-n *domain*	-D オプションで指定されるユーザーのドメイン。

オプション	説明
-w *password*	-D オプションで指定されるユーザーのパスワード。
-l *userid*	ユーザーのログイン ID。

次のオプションは任意です。

オプション	説明
-A [+ | -]*attributename*: *value*	変更する属性。*attributename* は LDAP スキーマで定義され、値により、ディレクトリのこの属性に指定された一部およびすべての現在の値が置き換えられます。同時に複数の属性を変更する場合、または同じ属性に複数の値を指定する場合は、このオプションを繰り返します。 *attributename* の前の「+」は、現在の属性リストに値が追加されることを示します。 「-」は値の削除を示します。 コマンド行にコマンドを指定し、「-」を使用する場合は、2 つの円記号を前に付けます。入力ファイル内でオプションを指定する場合、「-」記号の前に円記号を 1 つ付けます。
-d *domain*	ユーザーまたはグループのドメイン。-d を指定しない場合、-n で指定されるドメインが使用されます。
-h, -?	コマンド使用構文を印刷します。
-i *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
-p *AM port*	Access Manager が待機する代替 TCP ポートを指定します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
-s	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
-v	デバッグ出力を有効にします。
-V	ユーティリティーとそのバージョンに関する情報を印刷します。
-X *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

オプション	説明
-S *service*	ユーザーに -S オプションで指定されるサービスが割り当てられているかどうかを検証してから、指定されたサービスをユーザーに追加します。すでにユーザーにサービスが割り当てられている場合、エラーメッセージが表示されます。 *service* には単一のサービスまたは複数のサービスの値を指定できます。*service* に使用できる値は mail および cal です。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 -S mail,cal
次のオプションは、-S mail オプションを指定した場合にのみ使用できます。	
-E *email*	ユーザーの電子メールアドレスを指定します。
-H *mailhost*	ユーザーのメールホスト。 このオプションは、-S mail オプションが指定されている場合は必須です。
次のオプションは、-S cal オプションを指定した場合にのみ使用できます。	
-B *DWPHost*	このユーザーのカレンダをホスティングするバックエンドカレンダサーバーの DNS 名を指定します。 注: この属性は追加できますが、すでに存在する場合、変更できません。
-E *email*	カレンダユーザーの電子メールアドレスを指定します。
-J *First Day of Week*	カレンダサーバーのユーザーインタフェースにカレンダが表示されるときに示される最初の曜日。有効な値は 0 〜 6 (0 は日曜、1 は月曜...) です。

オプション	説明
-k *calid_type*	カレンダサービスを追加する場合は、作成されるカレンダ ID のタイプを指定します。使用できる値は legacy と hosted です。-k legacy を指定した場合、そのカレンダの ID のみが使用されます (例: jsmith)。-k hosted を指定した場合、そのカレンダの ID とドメインが使用されます (例: jsmith@sesta.com)。 -k オプションを指定しない場合は、デフォルトであるカレンダ ID とドメイン (hosted) が使用されます。 -k オプションを指定しない場合に作成されるカレンダ ID タイプの値を設定できます。これは、resource.properties ファイルに次のパラメータを追加して行います。 switch-caltype=*value* *value* は「hosted」または「legacy」です。 resource.properties ファイルは、次のディレクトリにあります。 *da_base*/data/WEB-INF/classes/sun/comm/cli/ \ server/servlet/resource.properties
-T *time zone*	ユーザーのカレンダはこのタイムゾーンに表示されます。 有効なタイムゾーンの文字列の一覧は、167 ページの「カレンダタイムゾーン文字列」を参照してください。

例

次の例では、メールサービスをユーザー smith に追加します。

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A description:"new description" -S mail -H mailhost.siroe.com
```

次の例では、メール転送アドレスをユーザー smith に追加します。

```
commadmin user modify -D chris -n sesta.com -w bolton -l smith \
-A +mailforwardingaddress:tsmith@siroe.com
```

commadmin user search

commadmin user search コマンドは、単一ユーザーに関連したすべてのディレクトリのプロパティーを取得します。複数のユーザーのディレクトリプロパティーをすべて取得する場合は、-i オプションを使用します。検索のあと、アクティブなユーザーのみが表示されます。

構文

`commadmin user search -D` *login* `-n` *domain* `-w` *password* `[-d` *domain*`] [-E` *string*`] [-F` *string*`]`

`[-h] [-?] [-i` *inputfile*`] [-L` *string*`] [-l` *string*`] [-p` *AM port*`] [-s] [-S` *service*`]`

`[-t` *Search Template*`] [-v] [-V] [-X` *AM host*`]`

オプション

次のオプションは必須です。

オプション	説明
`-D` *login*	このコマンドを実行する権限のあるユーザーのユーザー ID。
`-n` *domain*	`-D` オプションで指定されるユーザーのドメイン。
`-w` *password*	`-D` オプションで指定されるユーザーのパスワード。

次のオプションは任意です。

オプション	説明
`-d` *domain*	ユーザーのドメイン。ユーザーは指定されたドメイン内のみで検索されます。 `-d` を指定しない場合、すべてのドメインが検索対象と見なされます。
`-E` *string*	ユーザーのメールアドレスを検索します。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-F` *string*	ユーザーのファーストネームを検索します。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-h`, `-?`	コマンド使用構文を印刷します。
`-i` *inputfile*	コマンド行ではなく、ファイルからコマンド情報を読み取ります。
`-L` *string*	ユーザーの名字を検索します。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。
`-l` *string*	ユーザーのログイン名を検索します。文字列の任意の箇所にワイルドカード演算子 (*) を使用できます。

オプション	説明
`-p` *AM port*	このオプションは、Access Manager が待機する代替 TCP ポートを指定する場合に使用します。指定しない場合、デフォルトの *AM port* が使用されます。インストール時にデフォルトが設定されていない場合、ポート 80 が使用されます。
`-s`	SSL (Secure Socket Layer) を使用して Access Manager に接続します。
`-S` *service*	ユーザーの検索で一致させるサービスを指定します。 *service* には単一のサービスまたは複数のサービスの値を指定できます。*service* に使用できる値は `mail` および `cal` です。これらの値は大文字と小文字を区別しません。 サービスのリストはコンマ (,) 区切り文字で区切られます。 例 `-S mail,cal`
`-t` *Search template*	デフォルトの検索テンプレートの代わりに使用する検索テンプレートの名前を指定します。これはディレクトリ内で、検索用フィルタを定義するエントリです。アクティブなユーザーのみ検索されます。
`-v`	デバッグ出力を有効にします。
`-V`	ユーティリティーとそのバージョンに関する情報を印刷します。
`-X` *AM host*	Access Manager が実行されるホストを指定します。指定しない場合、デフォルトの *AM host* が使用されます。インストール時にデフォルトが設定されていない場合、ローカルホストが使用されます。

例

次の例では、`varrius.com` ドメインのユーザーが検索されます。

```
commadmin user search -D chris -w bolton -d varrius.com -n sesta.com
```

付録 A

サービスプロバイダ管理者とサービスプロバイダ組織

Delegated Administrator コンソールは、ディレクトリで作成できる新しいタイプの組織のほかに、新しい管理のロール、サービスプロバイダ管理者 (SPA) を提供します。

この付録では次の項目について説明します。

この付録では、サービスプロバイダ管理者のロールと新しい組織のタイプ、および Delegated Administrator でそれらを作成する方法について説明します。

サービスプロバイダ管理者

Delegated Administrator コンソールでは、新しいロールであるサービスプロバイダ管理者 (SPA) に管理作業を委任できます。SPA は新しいタイプの下位組織を作成し、管理できます。

SPA の権限範囲は、最上位管理者 (TLA) から組織管理者 (OA) までの間です。

SPA を設置することで、第 1 章の26 ページの「3 層階層」で説明した 3 層の管理階層を作成できます。

この第 2 レベルの委任により、大規模な LDAP ディレクトリでサポートされる大規模な顧客ベースの管理が軽減される場合があります。たとえば、ISP はそれぞれ独自の組織を必要とする数百または数千の小規模ビジネスにサービスを提供できます。毎日、数十の新しい組織をディレクトリに追加する必要も生じます。

2 層階層を使用する場合、TLA がこのような組織の新規作成をすべて担当することになります。3 層階層では TLA がこれらの作業を SPA に委任できます。

SPA は新規顧客のために下位組織を作成し、その下位組織のユーザーを管理する OA を割り当てられます。

図 A–1 に、3 層の組織階層サンプルの論理図を示します。

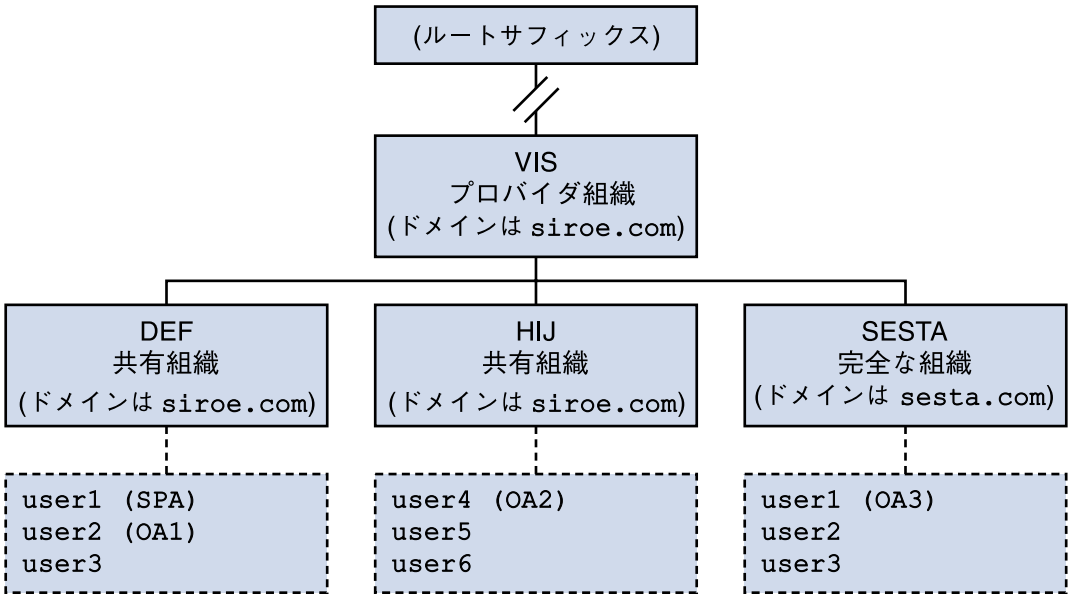

図 **A–1** サービスプロバイダ管理者を使用するディレクトリ: 論理図

図 A–1 の例では、プロバイダ組織が 1 つ示されています。ただし、1 つのディレクトリに複数のプロバイダ組織を格納できます。

この例では、管理作業は以下のように委任されます。

- SPA は、VIS プロバイダ組織およびその下にあるすべての組織を管理する権限を持っています。SPA のロールは、DEF 組織の `user1` に割り当てられています。
- 組織管理者 OA1 は、共有組織である DEF を管理します。この OA のロールは、DEF 組織の `user2` に割り当てられています。
- OA2 は共有組織 HIJ を管理します。この OA のロールは、HIJ 組織の `user4` に割り当てられています。
- OA3 は完全な組織 SESTA を管理します。この OA のロールは、SESTA 組織の `user1` に割り当てられています。

  SESTA は 1 つの完全な組織で、固有の名前空間を持っています。SESTA (`sesta.com` ドメイン内) の `user1` は固有のユーザー ID を持っています。

プロバイダと下位組織の定義については、145 ページの「サービスプロバイダ管理者で管理される組織」を参照してください。

サービスプロバイダ管理者のロール

SPA は次の作業を実行できます。

- SPA が管理権限を持つプロバイダ組織の、共有組織および完全な組織の作成、削除、変更。

  図 A–1 の例では、VIS プロバイダ組織の SPA は次の作業を実行できます。

  - DEF、HIJ、SESTA 組織の変更または削除。
  - VIS プロバイダ組織下の新規組織の作成。
- プロバイダ組織下のすべての組織のユーザーの作成、削除、変更。
- プロバイダ組織下のすべての組織のグループの作成、削除、変更。
- プロバイダ組織下のすべての組織のカレンダリソースの作成、削除、変更。
- ユーザーへの OA のロールの割り当て。

  たとえば、図 A–1 で示されるサンプル組織では、SPA は OA ロールを SESTA 組織の `user2` に割り当てることができます。その結果、`user2` は SESTA 組織のユーザーを管理できるようになります。

  SPA はユーザーから OA のロールを削除することもできます。
- プロバイダ組織下のほかの正当なユーザーに対する SPA のロールの割り当て (および SPA のロールの削除)。
- 組織へのサービスパッケージの割り当て。

  サービスパッケージの詳細については、第 1 章の 32 ページの「サービスパッケージ」を参照してください。

  SPA は指定されたタイプのサービスパッケージを組織に割り当て、各パッケージについて、その組織で使用できる数の上限を決定できます。

  たとえば、SPA は次のサービスパッケージを割り当てられます。

  - DEF 組織

    ```
    1,000 gold パッケージ
    500 platinum パッケージ
    ```

  - HIJ 組織

    ```
    2,500 topaz パッケージ
    500 platinum パッケージ
    500 emerald パッケージ
    1,000 ruby パッケージ
    ```

  - SESTA 組織

    ```
    2,000 silver パッケージ
    1,500 gold パッケージ
    100 platinum パッケージ
    ```

    SPA は Delegated Administrator コンソールを使用して上記のタスクを実行できます。このリリースでは、Delegated Administrator ユーティリティーには上記のタスクを実行するコマンドオプションは含まれていません。

注 – TLA は既存の共有組織、または完全な組織の変更や削除ができます。TLA は、これらの組織のユーザーも管理できます。

TLA はユーザーから SPA のロールを削除することはできますが、コンソールから SPA のロールを割り当てることはできません。このリリースの Delegated Administrator の制約については、144 ページの「このリリースに関する注意点」を参照してください。

TLA によって実行される管理作業の詳細については、第 1 章の 27 ページの「管理者のロールとディレクトリ階層」を参照してください。

ユーザーに SPA のロールを割り当てる

SPA のロールは、SPA に指定された組織と、SPA が管理するプロバイダ組織の下位組織のユーザーに割り当てる必要があります。

図 A–1 の例では、VIS プロバイダ組織に SPA を作成する必要があると想定します。SPA のロールを DEF 組織の `user1` に割り当てます。

プロバイダ組織のノードにはユーザーが含まれていないため、SPA は下位組織に存在している必要があります。

したがって、SPA がプロバイダ組織を管理するためには、その下に少なくとも 1 つの組織を作成する必要があります。この組織を、SPA のロールを割り当てるユーザーが所属する組織として指定します。詳細については、146 ページの「プロバイダ組織とサービスプロバイダ管理者の作成」を参照してください。

このリリースに関する注意点

このリリースの Delegated Administrator では、Delegated Administrator コンソールまたはユーティリティーを使用して SPA やプロバイダ組織を作成できません。

SPA やプロバイダ組織を作成するには、サービスプロバイダのカスタムテンプレートである `da.provider.skeleton.ldif` を手動で変更する必要があります。

サービスプロバイダのカスタムテンプレートを使用してこれらの作業を実行する手順については、この付録で後述する 146 ページの「プロバイダ組織とサービスプロバイダ管理者の作成」を参照してください。

サービスプロバイダ管理者で管理される組織

SPA は SPA のプロバイダ組織下にある次のタイプの組織を作成、変更、および削除できます。

- 145 ページの「完全な組織」
- 146 ページの「共有組織」

プロバイダ組織、完全な組織、共有組織について次の各項で説明します。

プロバイダ組織

プロバイダ組織は、完全な組織と共有組織を論理的に格納する LDAP ディレクトリ内のノードです。プロバイダ組織のノードには、SPA による下位組織の管理を可能にする属性が備わっています。

LDAP ディレクトリでは、プロバイダ組織をメールドメインの下に置く必要があります。この付録で後述する161 ページの「サービスプロバイダ組織のサンプルデータ」に例を示します。

プロバイダ組織はユーザーエントリを格納できません。その代わり、ユーザーはプロバイダ組織下に作成された組織でプロビジョニングされます。

プロバイダ組織は、プロバイダ組織下に作成された組織に関するディレクトリ情報を格納します。次に例を示します。

- プロバイダ組織下に格納される組織の種類、すなわち共有組織、完全な組織、両方の組織のいずれか。
- このプロバイダ組織内で作成された共有組織が使用できるドメイン名。
- このプロバイダ組織内で作成された組織が利用できる、サービスクラスパッケージのタイプと数。
- プロバイダ組織の SPA が所属する組織。

完全な組織

完全な組織には次の特徴があります。

- プロバイダ組織の下位組織であり、SPA により作成されます。
- ユーザーは完全な組織でプロビジョニングされます。

  図 A–1 に示す例では、`user2` は `sesta.com` ドメインに所属し、`user2@sesta.com` というメールアドレスを持ちます。

- 完全な組織は、ほかの組織が共有することができない独自のドメインと固有の名前空間を持っています。

  図 A–1 に示す例では、完全な組織である SESTA のドメイン名は `sesta.com` です。

共有組織

共有組織には次の特徴があります。

- プロバイダ組織の下位組織であり、SPA により作成されます。
- ユーザーは共有組織でプロビジョニングされます。

  図 A–1 に示す例では、 `user5` は `siroe.com` ドメインに所属し、`user5@siroe.com` というメールアドレスを持ちます。
- プロバイダ組織が提供するリストの 1 つまたは複数の共有ドメイン名を使用します。

  図 A–1 に示す例では、共有組織 DEF はドメイン名 `siroe.com` を使用します。
- ほかの共有組織は、この組織が使用するドメイン名を共有できます。

  図 A–1 に示す例では、DEF と HIJ の両方の組織が `siroe.com` ドメインに所属します。
- 共有組織には固有の名前空間がありません。

プロバイダ組織とサービスプロバイダ管理者の作成

このリリースの Delegated Administrator では、Delegated Administrator が提供するサービスプロバイダのカスタムテンプレート (`da.provider.skeleton.ldif`) を使用して、独自のプロバイダ組織と SPA を作成する必要があります。

注 – Delegated Administrator の設定プログラムを実行する際に、サンプルのプロバイダ組織 (下位組織を含む) とサンプルの SPA をディレクトリにインストールすることもできます。それには、設定プログラムで「サンプル組織を読み込む」を選択します。

ただし、サンプル組織のテンプレート (`da.sample.data.ldif`) はサンプルとして使用されるものであり、独自のプロバイダ組織を作成するためのテンプレートではありません。このサンプルの詳細については、この付録の後半の 161 ページの「サービスプロバイダ組織のサンプルデータ」を参照してください。

プロバイダ組織と SPA を作成すると、その SPA はDelegated Administrator コンソールにログインして下位組織を作成および管理できます。 また、その SPA の組織内のユーザーに SPA のロールを割り当てることができます。ただし、これらの SPA が管理できるのは同じプロバイダ組織だけです。

別のプロバイダ組織とそれを管理する SPA を作成するには、改めてサービスプロバイダのカスタムテンプレートを使用する必要があります。

ここで説明する内容は次のとおりです。

- 147 ページの「テンプレートによって作成されるエントリ」では、編集済みのテンプレートのコピーをディレクトリにインストールするときに作成される組織の例を示します。
- 148 ページの「プロバイダ組織、下位組織、SPA を作成するために必要な情報」では、プロバイダ組織、共有の下位組織、および SPA の作成に必要なテンプレート内のパラメータを定義します。
- 153 ページの「プロバイダ組織とサービスプロバイダ管理者を作成する手順」では、テンプレートの編集方法とディレクトリへの情報のインストール方法を説明します。
- 154 ページの「サービスプロバイダのカスタムテンプレート」では、テンプレートの一覧を示します。

テンプレートによって作成されるエントリ

サービスプロバイダのカスタムテンプレートの編集済みコピーをディレクトリにインストールすると、次のエントリが作成されます。

- プロバイダ組織。
- SPA が所属する下位の共有組織。
- SPA のロールを割り当てられる下位組織のユーザー1名。
- 完全な組織を作成できるプレースホルダのノード。プロバイダ組織の SPA がこの完全な組織を管理します。

図 A–2 に、テンプレートのインストール時に作成されるエントリの例を示します。これを組織のディレクトリ情報ツリー (DIT) と呼びます。

図 A–2 は一例です。組織名、SPA ユーザー名、DIT 構成は組織によって異なります。

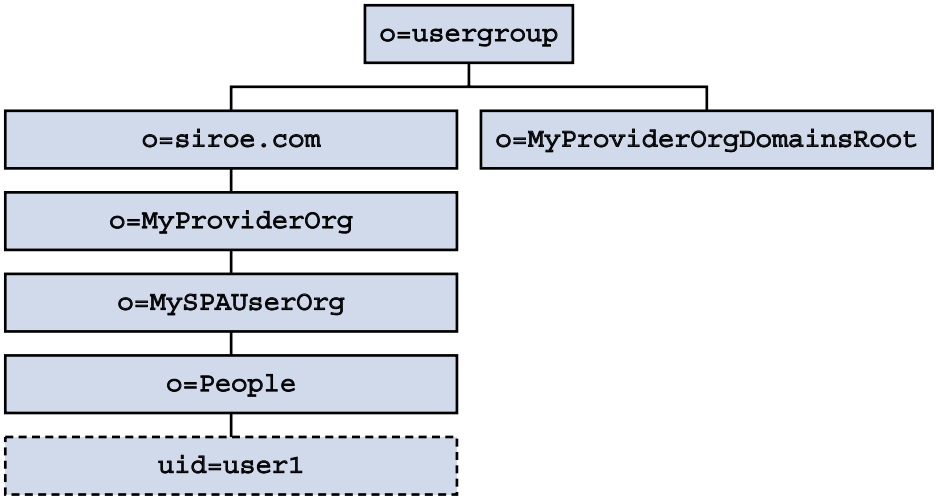

図 **A–2** サービスプロバイダのカスタムテンプレート: ディレクトリ情報ツリー図

サンプルとしてインストールしたサービスプロバイダのカスタムテンプレートのノード

図 A–2 に示す例のノードは次のとおりです。

- `o=usergroup` - ユーザー/グループデータのルートサフィックス。
- `o=siroe.com` - プロバイダ組織が使用するメールドメイン。
- `o=MyProviderOrg` - プロバイダ組織のノード。
- `o=MySPAUserOrg` - プロバイダ組織のユーザー (SPA のロールが割り当てられるユーザーを含む) が所属する下位の共有組織。
- `ou=people` - ユーザーの格納に必要な標準 LDAP 組織単位。
- `uid=user1` - MySPAUserOrg 組織で SPA になるユーザーの uid。
- `o=MyProviderOrgDomainsRoot` - MyProviderOrg プロバイダ組織の下位にある完全な組織を保持するプレースホルダノード。

プロバイダ組織、下位組織、SPA を作成するために必要な情報

プロバイダ組織、1 つの下位組織、1 名の SPA を作成するには、組織の形態に応じてサービスプロバイダのカスタムテンプレートのパラメータを書き換える必要があります。

各パラメータについては、154 ページの「サービスプロバイダのカスタムテンプレート」に示す `da.provider.skeleton.ldif` の一覧を参照してください。または、次のディレクトリにある ldif ファイルを開いてください。

da_base`/lib/config-templates`

これらのパラメータに関連づけられた属性の定義については、『*Sun Java System Communications Services Schema Reference*』の第 5 章「Communications Services Delegated Administrator Classes and Attributes (Schema 2)」および第 3 章「Messaging Server and Calendar Server Attributes」を参照してください。

プロバイダ組織と下位組織を定義するパラメータ

プロバイダ組織と下位組織を作成するには、次のパラメータを編集します。

- *ugldapbasedn*

  ディレクトリのユーザーデータとグループデータのルートサフィックス

  例

  ```
  o=usergroup
  ```

  ```
  dc=red,dc=iplanet,dc=com
  ```

- *maildomain_dn*

  メールドメインの完全な DN で、この下にプロバイダ組織が作成されます。

  例

  ```
  o=siroe.com, o=usergroup
  ```

  ```
  o=sesta.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

- *maildomain_dn_str*

  すべてのコンマ (,) を下線 (_) で置き換えたメールドメイン DN。

  たとえば、メールドメイン DN が次のような場合を考えます。

  ```
  o=siroe.com,o=SharedDomainsRoot,o=Business,dc=red, \
  dc=iplanet,dc=com
  ```

  メールドメイン DN の文字列は次のようになります。

  ```
  o=siroe.com_o=SharedDomainsRoot_o=Business_dc=red_ \
  dc=iplanet_dc=com
  ```

- *providerorg*

  プロバイダ組織の名前。プロバイダ組織が存在するディレクトリノードが、この名前になります。

  このパラメータは、テンプレート `da.provider.skeleton.ldif` で繰り返し使用されます。

  例

  ```
  sunProviderOrgDN: o=MyProviderOrg,o=siroe.com,o=usergroup
  ```

```
o=MyProviderOrg

sunBusinessOrgBase: o=MyProviderOrgdomainsroot, o=usergroup
```

- *servicepackage*

  プロバイダ組織の下位組織のユーザーに割り当てるサービスパッケージの名前。これは、多値パラメータです。

  da.provider.skeleton.ldif ファイルの「Provider Organization」の項には、次の属性があります。

  ```
  sunIncludeServices: <servicepackage>
  ```

  プロバイダ組織にサービスパッケージを含めるときは、属性 sunIncludeServices のインスタンス 1 つとパラメータ *servicepackage* を追加します。下位組織のユーザーには、ここに記述したサービスパッケージのみ割り当てられます。

  例

  ```
  sunIncludeServices: gold
  sunIncludeServices: platinum
  sunIncludeServices: ruby
  sunIncludeServices: silver
  ```

  属性 sunIncludeServices を使用しない場合 (パラメータ *servicepackage* が含まれている行を削除した場合) は、ディレクトリ内のすべてのサービスパッケージを割り当てることができます。

- *domain_name*

  プロバイダ組織の下位組織に割り当てられるドメイン名。これは、多値パラメータです。

  da.provider.skeleton.ldif ファイルの「Provider Organization」の項には、次の属性があります。

  ```
  sunAssignableDomains: <domain_name>
  ```

  属性 sunAssignableDomains のドメイン名は、メールドメイン組織の属性 sunPreferredDomain と属性 associatedDomain に記述した名前の一部 (または全部) です。メールドメイン組織の下にプロバイダ組織が作成されます。

  プロバイダ組織にドメイン名を含めるときは、属性 sunAssignableDomains のインスタンス 1 つと、パラメータ *domain_name* を追加します。下位組織には、ここに記述したドメイン名だけが割り当てられます。

  例

  ```
  sunAssignableDomains: siroe.com
  sunAssignableDomains: siroe.net
  sunAssignableDomains: varrius.com
  sunAssignableDomains: sesta.com
  sunAssignableDomains: sesta.net
  ```

- *provider_sub_org*

  SPA ユーザーが所属する共有組織の名前。編集した ldif の情報をディレクトリにインストールすると、プロバイダ組織の下に共有組織が作成されます。この組織は、SPA ユーザーが所属する組織として指定されます。プロバイダ組織の SPA に

なるほかのユーザーも、すべてこの共有組織に所属する必要があります。

da.provider.skeleton.ldif ファイルの「Provider Organization」の項には、次の属性があります。

```
sunProviderOrgDN:
o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
```

属性 sunProviderOrgDN は、プロバイダ組織ユーザーの中でも、特に SPA ユーザーが所属する組織を識別します。

例

```
sunProviderOrgDN:
o=MySPAUserOrg,o=MyProviderOrg,o=siroe.com,o=usergroup
```

- *preferredmailhost*

  SPA ユーザーが所属するプロバイダ組織の、下位組織のメールホストにするマシンの名前。必ず完全修飾ドメイン名 (FQDN) を使用します。

  da.provider.skeleton.ldif ファイルの「Shared Subordinate Organization」の項には、次の属性があります。

  ```
  preferredMailHost: <preferredmailhost>
  ```

  例

  ```
  preferredMailHost: mail.siroe.com
  ```

- *available_domain_name*

  特定の下位組織のユーザーに割り当てられるドメイン名。これは、多値パラメータです。

  available_domain_name の値は、属性とパラメータ sunAssignableDomains: <domain_name> に与えられた値の一部です。*domain_name* がプロバイダ組織全体に適用されるのに対し、*available_domain_name* は 1 つの下位組織に適用されます。

  da.provider.skeleton.ldif ファイルの「Shared Subordinate Organization」の項には、次の属性があります。

  ```
  sunAvailableDomainNames: <available_domain_name>
  ```

  プロバイダ組織の属性 sunAssignableDomains から下位組織に継承するドメイン名ごとに、属性 sunAvailableDomains のインスタンス 1 つとパラメータ*available_domain_name* を追加します。下位組織には、ここに記述したドメイン名だけが割り当てられます。

  例

  ```
  sunAvailableDomainNames: siroe.com
  sunAvailableDomainNames: siroe.net
  sunAvailableDomainNames: varrius.com
  ```

- *available_services*

  特定の下位組織で使用可能なサービスパッケージ。これは、多値パラメータです。

  下位組織に割り当てるサービスパッケージは、属性 sunIncludeServices でプロバイダ組織全体に割り当てたパッケージの一部です。

`da.provider.skeleton.ldif` ファイルの「Shared Subordinate Organization」の項には、次の属性があります。

```
sunAvailableServices: <available_services>
```

パラメータ *available_services* の形式は次のとおりです。

service package name: count

count は整数で指定します。数を指定しないと、無制限になります。

プロバイダ組織の属性 `sunIncludeServices` から下位組織に継承するサービスパッケージごとに、属性 `sunAvailableServices` のインスタンス 1 つとパラメータ *available_services* を追加します。

例

```
sunAvailableServices: gold:1500
sunAvailableServices: platinum:2000
sunAvailableServices: silver:5000
```

SPA を定義するパラメータ

SPA を作成するには、次のパラメータを編集します。

- *spa_uid*

  SPA ユーザーのユーザーID。

  例

  ```
  uid: user1
  ```

- *spa_password*

  SPA ユーザーのパスワード。

  例

  ```
  userPassword: x12P3&qrS
  ```

- *spa_firstname*

  SPA ユーザーのファーストネーム。

  例

  ```
  givenname: John
  ```

- *spa_lastname*

  SPA ユーザーのラストネーム。

  例

  ```
  sn: Smith
  ```

- *spa_servicepackage*

  SPA ユーザーに割り当てられたサービスパッケージ。サービスパッケージの詳細については、第 1 章の 32 ページの「サービスパッケージ」を参照してください。

  例

```
inetCos: platinum
```

- *spa_mailaddress*

  SPA ユーザーの電子メールアドレス。メールアドレスのドメイン部分は、必ず *available_domain_name* のパラメータとして設定したドメイン値の中の 1 つになります。すなわち、必ず SPA ユーザーが所属する下位組織に割り当てられたドメインになります。詳細については、149 ページの「プロバイダ組織と下位組織を定義するパラメータ」を参照してください。

  例

  ```
  mail: user1@siroe.com
  ```

サービスプロバイダのカスタムテンプレートを編集し、その情報をディレクトリにインストールする方法については、153 ページの「プロバイダ組織とサービスプロバイダ管理者を作成する手順」を参照してください。

プロバイダ組織とサービスプロバイダ管理者を作成する手順

ldif ファイルの `da.provider.skeleton.ldif` を使用して、次の手順を実行します。

▼ プロバイダ組織とサービスプロバイダ管理者を作成する

手順

1. ディレクトリにメールドメインを作成します。

   まだメールドメインを作成していない場合は、ディレクトリにメールドメインを作成します。プロバイダ組織と下位の共有組織は、このメールドメインを使用します。

2. **`da.provider.skeleton.ldif`** ファイルをコピーし、名前を変更します。

   Delegated Administrator をインストールすると、`da.provider.skeleton.ldif` ファイルが次のディレクトリにインストールされます。

   da_base `/lib/config-templates`

3. **`da.provider.skeleton.ldif`** ファイルのコピーの次のパラメータを編集します。これらのパラメータを、インストールする値で書き換えます。

   パラメータの定義については、148 ページの「プロバイダ組織、下位組織、SPA を作成するために必要な情報」を参照してください。

   パラメータの中には、ldif ファイルの中で何度も使用されるものがあります。各パラメータのすべてのインスタンスを検索し、書き換えてください。

   多値属性の値を表すパラメータもあります。これらのパラメータを関連する属性名と共にコピーして編集すると、ldif ファイルに複数のインスタンスを作成できます。多値パラメータを、次に示します。

- <ugldapbasedn>
- <maildomain_dn>
- <maildomain_dn_str>
- <providerorg>
- <servicepackage> (多値)
- <domain_name> (多値)
- <provider_sub_org>
- <preferredmailhost>
- <available_domain_name> (多値)
- <available_services> (多値)
- <spa_uid>
- <spa_password>
- <spa_firstname>
- <spa_lastname>
- <spa_servicepackage>
- <spa_mailaddress>

  これらのパラメータに関連づけられた属性の定義については、『*Sun Java System Communications Services Schema Reference*』の第 5 章「Communications Services Delegated Administrator Classes and Attributes (Schema 2)」および第 3 章「Messaging Server and Calendar Server Attributes」を参照してください。

4. **LDAP** ディレクトリツール **`ldapmodify`** を使用して、プロバイダ組織と **SPA** をディレクトリにインストールします。

   コマンド実行の例を次に示します。

   ```
   ldapmodify -D <directory manager> -w <password> \
   -f <da.provider.finished.ldif>
   ```

   各表記の意味は次のとおりです。

   <directory manager> は Directory Server 管理者の名前です。

   <password> は Directory Service 管理者のパスワードです。

   <da.provider.finished.ldif> は、新しいプロバイダ組織と SPA としてディレクトリにインストールされる編集済み ldif ファイルの名前です。

サービスプロバイダのカスタムテンプレート

このテンプレート (da.provider.skeleton.ldif) には、新しいプロバイダ組織と SPA を作成するために書き換える必要があるパラメータが含まれます。

次に、ldif ファイルの中でパラメータを持つ部分を示します。これがファイルのすべてではありません。Access Manager 対応に必要なエントリとACIが、ここには含まれていません。

ldif ファイルの中のパラメータだけを変更してください。Access Manager に関連する項目は変更しないでください。

da.provider.skeleton.ldif File (関連項目)

```
#
# The following parameterized values must be replaced.
#
# <ugldapbasedn>          :: Root suffix for user/group data
# <maildomain_dn>         :: Complete dn of the mail domain underneath
#                            which the provider organization will be
#                            created.
# <maildomain_dn_str>     :: The maildomain dn with all ',' replaced
#                                      by '_'. E.g.
#                            dn --\> o=siroe.com,o=SharedDomainsRoot,
#                            o=Business,dc=red,dc=iplanet,dc=com
#                            dn_str --> o=siroe.com_o=SharedDomainsRoot_
#                            o=Business_dc=red_dc=iplanet_dc=com
# <providerorg>            : Organization value for provider node.
# <servicepackage>        :: One for each service package to include.
#                            All service packages in the system
#                            may be assigned by leaving this value empty.
# <domain_name>           :: One for each DNS name which may be assigned
#                            to a subordinate organization.
#                            These names form a proper subset (some or
#                            all) of the names listed in the <maildomain>
#                            organization's sunpreferreddomain
#                            and associateddomain attributes.
# <provider_sub_org>      :: Organization value for the shared subordinate
#                            organization in which the Provider
#                            Administrator resides.
# <preferredmailhost>     :: Name of the preferred mail host for the
#                            provider's subordinate organization.
# <available_domain_name> :: one for each DNS name that an organization
#                            allows an organization admin to use when
#                            creating a user's mail address.  This is
#                            a proper subset of the values given for
#                            <domain_name> (sunAssignableDomains attribute).
# <available_services>    :: One for each service packags available to an
#                            organization (sunAvailableServices attribute).
#                            These service packages form a proper subset
#                            of the ones assigned to a provider organization
#                            - <servicepackage> (sunIncludeServices
#                            attribute).  Form is
#                            <service package name>:<count>
#                            where count is an integer.  If count is absent
#                            then default is unlimited.
# <spa_uid>               :: The uid for the service provider administrator.
```

```
# <spa_password>          :: The password for the service provider
#                            administrator.
# <spa_firstname>         :: First name of the service provider
#                            administrator.
# <spa_lastname>          :: Last name of the service provider
#                            administrator.
# <spa_servicepackage>    :: Service package assigned to the service
#                            provider administrator.
# <spa_mailaddress>       :: The spa's mail address. The domain part of the
#                            mail address must be one of the values used for
#                            <available_domain_name>.
#


#
# Provider Organization
#
dn: o=<providerorg>,<maildomain_dn>
changetype: add
o: <providerorg>
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunManagedProvider
sunAllowBusinessOrgType: full
sunAllowBusinessOrgType: shared
sunBusinessOrgBase: o=<providerorg>domainsroot,<ugldapbasedn>
sunIncludeServices: <servicepackage>
sunAssignableDomains: <domain_name>
sunAllowMultipleDomains: true
sunAllowOutsideAdmins: false
sunProviderOrgDN: o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# Full Organizations node
#
dn: o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
o: <providerorg>DomainsRoot
objectClass: top
objectClass: organization
objectClass: sunmanagedorganization
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
```

```
# Provider Admin Role shared organizations
#
dn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Provider Admin Role full organizations
#
dn: cn=Provider Admin Role,o=<providerorg>DomainsRoot,<ugldapbasedn>
changetype: add
cn: Provider Admin Role
objectClass: ldapsubentry
objectClass: nssimpleroledefinition
objectClass: nsroledefinition
objectClass: nsmanagedroledefinition
objectClass: iplanet-am-managed-role
objectClass: top
iplanet-am-role-description: Provider Admin

#
# Shared Subordinate Organization. Includes 1 user who is
# the Provider Administrator.
#
dn: o=<provider_sub_org>,=<providerorg>,<maildomain_dn>
changetype: add
preferredMailHost: <preferredmailhost>
sunNameSpaceUniqueAttrs: uid
o: <provider_sub_org>
objectClass: inetdomainauthinfo
objectClass: top
objectClass: sunismanagedorganization
objectClass: sunnamespace
objectClass: sunmanagedorganization
objectClass: organization
objectClass: sunDelegatedOrganization
objectClass: sunMailOrganization
sunAvailableDomainNames: <available_domain_name>
sunAvailableServices: <available_services>
sunOrgType: shared
sunMaxUsers: -1
sunNumUsers: 1
sunMaxGroups: -1
sunNumGroups: 0
sunEnableGAB: true
sunAllowMultipleServices: true
inetDomainStatus: active
sunRegisteredServiceName: GroupMailService
```

```
sunRegisteredServiceName: DomainMailService
sunRegisteredServiceName: UserMailService
sunRegisteredServiceName: iPlanetAMAuthService
sunRegisteredServiceName: UserCalendarService
sunRegisteredServiceName: iPlanetAMAuthLDAPService
sunRegisteredServiceName: DomainCalendarService
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

dn: ou=People,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: People
objectClass: iplanet-am-managed-people-container
objectClass: organizationalUnit
objectClass: top

dn: ou=Groups,o=<provider_sub_org>,o=<providerorg>,<maildomain_dn>
changetype: add
ou: Groups
objectClass: iplanet-am-managed-group-container
objectClass: organizationalUnit
objectClass: top
# .
# .
# [Entries and ACIs required by Access Manager]
# .
# .

#
# User - provider administrator
#
dn: uid=<spa_uid>,ou=People,o=<provider_sub_org>,o=<providerorg>, \
        <maildomain_dn>
changetype: add
sn: <spa_lastname>
givenname: <spa_firstname>
cn:  <spa_firstname> <spa_lastname>
uid: <spa_uid>
iplanet-am-modifiable-by: cn=Top-level Admin Role,<ugldapbasedn>
objectClass: inetAdmin
objectClass: top
objectClass: iplanet-am-managed-person
objectClass: iplanet-am-user-service
objectClass: iPlanetPreferences
objectClass: person
objectClass: organizationalPerson
objectClass: inetuser
objectClass: inetOrgPerson
objectClass: ipUser
objectClass: inetMailUser
objectClass: inetLocalMailRecipient
objectClass: inetSubscriber
```

```
objectClass: userPresenceProfile
objectClass: icsCalendarUser
mailhost: <preferredmailhost>
mail: <spa_mailaddress>
maildeliveryoption: mailbox
mailuserstatus: active
inetCos: <spa_servicepackage>
inetUserStatus: Active
nsroledn: cn=Provider Admin Role,o=<providerorg>,<maildomain_dn>
userPassword: <spa_password>
```

共有および完全な下位組織の作成

プロバイダ組織と SPA を作成したら、SPA はプロバイダ組織の下位となる共有組織と完全な組織の両方を作成し、管理できるようになります。SPA は Delegated Administrator コンソールを使用して、これらの作成作業を実行します。

次の作業は、共有組織または完全な組織を作成するための主要なステップの概要を示します。この作業では、「新しい組織を作成」ウィザードを使用して組織を作成するときに表示される情報の入力方法をすべて説明しているわけではありません。「新しい組織を作成」ウィザードの詳細については、Delegated Administrator コンソールのオンラインヘルプを参照してください。

▼ 共有または完全な下位組織を作成する

手順 **1. Delegated Administrator** コンソールを起動します。

次の URL に進みます。

`http://`*host*`:`*port*`/da/DA/Login`

各表記の意味は次のとおりです。

host は Web コンテナのホストマシンです。

port は Web コンテナのポートです。

次に例を示します。

```
http://siroe.com:8080/da/DA/Login
```

Delegated Administrator コンソールのログインウインドウが表示されます。

2. **SPA** のログイン **ID** とパスワードを使用して **Delegated Administrator** コンソールにログインします。

   SPA の作成方法については、すでに146 ページの「プロバイダ組織とサービスプロバイダ管理者の作成」で説明しています。

   「サービスプロバイダ管理者」ページが表示されます。デフォルトで「組織」タブが選択されています。このページには、SPA のプロバイダ組織の下位組織が表示されます。

3. 「新規組織」をクリックします。

   「新しい組織を作成」ウィザードが表示されます。「新しい組織を作成」ウィザードでの情報の入力方法と選択方法については、Delegated Administrator コンソールのオンラインヘルプを参照してください。

4. 「組織情報」パネルに情報を入力し、「次へ」をクリックします。

   「連絡先情報」パネルが表示されます。

5. 「連絡先情報」パネルに情報を入力し、「次へ」をクリックします。

   「アカウント情報」パネルが表示されます。

6. 共有組織または完全な組織を作成するかどうかを選択します。

   「アカウント情報」パネルで、新しい組織を共有組織とするか完全な組織とするかを決定します。

   共有組織は、ほかの組織と共有される既存のドメインを使用します。

   完全な組織は独自の固有ドメインを持ちます。

   - 共有組織を作成するには、「利用可能なドメインから選択」ラジオボタンをクリックします。

     ドロップダウンリストからドメインを選択します。

     注 – 共有組織の作成時には、カレンダサービスの詳細が既存の親ドメインから継承されます。したがって、新しい組織のためにカレンダサービスの情報を入力することはありません。「新しい組織を作成」ウィザードに「カレンダサービスの詳細」パネルは表示されません。さらに、共有組織の作成後は、「カレンダサービスの詳細」は組織の「プロパティー」ページに表示されません。

   - 完全な組織を作成するには、「新しいドメイン」ラジオボタンをクリックします。

     テキストボックスに新しいメールドメイン名を入力します。例 : `siroe.com`

     必要に応じて、「新しいドメインのエイリアス名」テキストボックスに新しいドメインのエイリアス名を入力します。

7. 「新しい組織を作成」ウィザードの残りのパネルで情報を入力します。

   後続のパネルの詳細については、Delegated Administrator コンソールのオンラインヘルプを参照してください。

サービスプロバイダ組織のサンプルデータ

Delegated Administrator 設定プログラム `config-commda` の実行時に、サンプル組織データ (ldif ファイルで定義) をディレクトリにインストールすることを選択できます。設定プログラムを実行するときに、「サービスパッケージと組織のサンプル」パネルで「サンプル組織を読み込む」を選択してください。設定プログラムによって、`da.sample.data.ldif` ファイルが LDAP ディレクトリツリーに追加されます。

この ldif ファイルはサンプルであり、実際にプロバイダ組織を作成するためのテンプレートではありません。新しいプロバイダ組織を作成するには、148 ページの「プロバイダ組織、下位組織、SPA を作成するために必要な情報」を参照してください。

サンプルデータで提供される組織

図 A–1 には、サンプル ldif ファイルによって提供される組織構造の論理図が示されています。ただし、図 A–1 には、ファイルに存在しない共有組織 HIJ が追加されています。

サンプル ldif ファイルでは、ルートサフィックスノード内に次の組織が格納されます。

- VIS プロバイダ組織。VIS プロバイダ組織の SPA は、次の組織を管理します。
  - 完全な組織、SESTA。SESTA 組織は独自のドメイン `sesta.com` を持ちます。
  - 共有組織、DEF。DEF 組織は共有ドメイン `siroe.com` を使用します。
- ESG プロバイダ組織。このプロバイダ組織には、下位組織が定義されていません。

この ldif ファイルは、次のように組織の管理者のロールを定義します。

- VIS プロバイダ組織の SPA (`user2@abc.com`)
- ESG プロバイダ組織の SPA (`user2_def`)
- SESTA 組織の OA (`user1@abc.com`)
- DEF 組織の OA (`user1_def`)

論理階層とディレクトリ情報ツリー

3 層ディレクトリ階層では、ディレクトリ情報ツリー (DIT) は 図 A–1 に示される論理図とは厳密には一致しません。組織は部分的に異なる階層の DIT で実装されます。

たとえば、DIT では完全なドメインはルートサフィックス直下に存在する必要があります。したがって、ドメインノードはルートサフィックスの下に追加され、共有ドメイン (共有組織で使用) と、完全な組織 (独自のドメインを保有) の LDAP 情報を格納します。

サンプル組織データ: ディレクトリ情報ツリー図

図 A–3 に、サンプル組織データのディレクトリ情報ツリー (DIT) の図を示します。

図 A–3 に示す例は、図 A–1 の論理図と同様に次の組織が含まれます。

- VIS と ESG (プロバイダ組織)
- DEF、VIS プロバイダ組織の下位にある共有組織
- SESTA、VIS プロバイダ組織の下位にある完全な組織

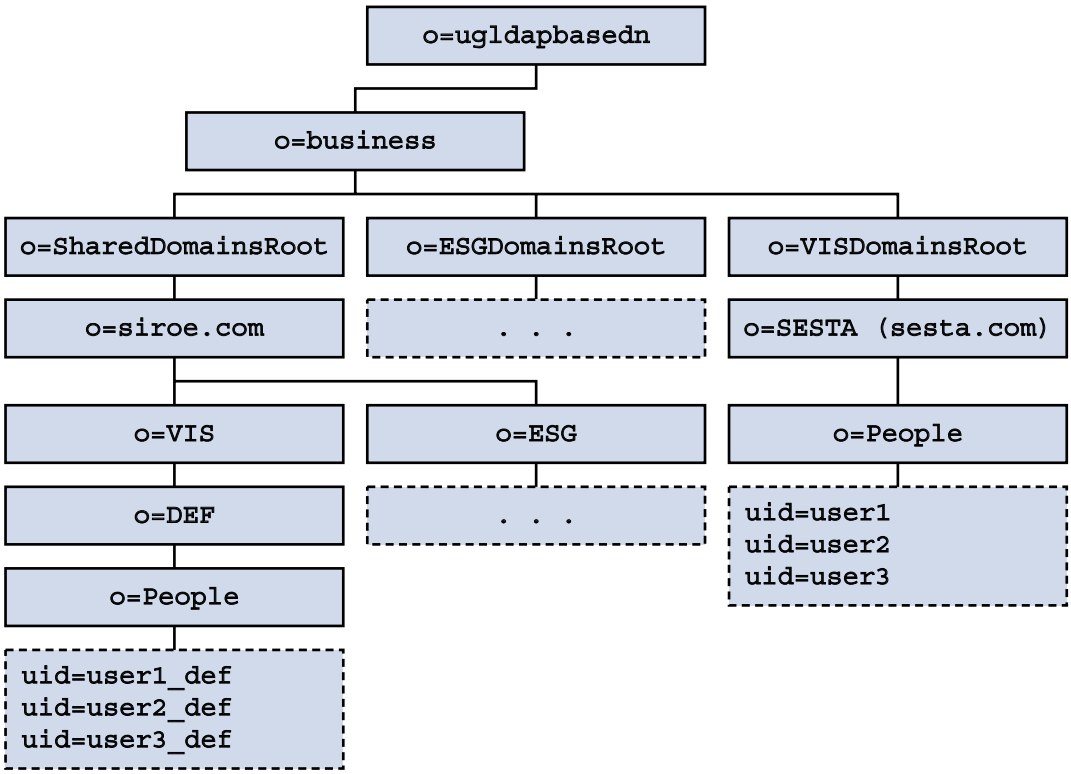

図 **A–3** サンプル組織データ: ディレクトリ情報ツリー図

サンプルディレクトリ情報ツリーのノード

サンプル組織ファイル (`da.sample.data.ldif`) のノードは次のとおりです。

- *ugldapbasedn* - このパラメータはルートサフィックスを表します。
- `o=business` - ディレクトリのすべてのビジネスを納めたノード。
- `o=SharedDomainsRoot` - 共有組織で使用されるドメインを格納するためのノード。

  このディレクトリ情報ツリーでは、異なるサービスプロバイダ組織の下位にある共有組織は、同じ共有ドメインを使用できます。これは、両方のプロバイダ組織が `SharedDomainsRoot` ノードの下にノードを保有するためです。
- `o=ESGDomainsRoot` と `o=VISDomainsRoot` - これらのノードには、ESG と VIS の両プロバイダ組織下に作成されるすべての完全な組織が格納されます。

  完全な組織を管理する各プロバイダ組織は、このレベル (ルートサフィックス下) でノードを保有する必要があります。

それぞれが独自のドメインを保有する複数の完全な組織は、ESGDomainsRoot または VISDomainsRoot の下に存在できます。

- o=siroe.com - 共有ドメイン。共有組織、DEF で使用されます。
- o=VIS と o=ESG - これらのプロバイダ組織のノードには、VIS と ESG の両プロバイダ組織下に作成されたすべての共有組織が格納されます。

  たとえば共有組織 DEF は、VIS プロバイダ組織の下位組織です。
- o=SESTA - 完全な組織。独自のドメイン sesta.com を持ちます。
- o=DEF - 共有組織。ドメイン siroe.com を使用します。
- ou=people - ユーザーの格納に必要な標準 LDAP 組織単位。

サンプルディレクトリ情報ツリーのユーザー *DN*

図 A–3 に示すサンプル組織ファイルの一部のユーザー DN は、次のとおりです。

- DEF 組織に所属するユーザー user1_def

  dn: uid=user1_def,ou=People,o=DEF,o=VIS,o=siroe.com,
  o=SharedDomainsRoot,o=Business,*ugldapbasedn*
- SESTA 組織に所属するユーザー user1

  dn: uid=user1,ou=People,o=SESTA,o=VISDomainsRoot,
  o=Business,*ugldapbasedn*

付録 B

属性値とカレンダタイムゾーン

属性値

表 B–1 に示す属性は、次のコマンドで -P オプションとともに使用できます。102 ページの「commadmin domain create」 と 107 ページの「commadmin domain modify」 です。属性はビット対応型の属性か複数値の属性のいずれかになります。

表 **B–1** -P オプションの属性

属性	値	説明
createLowerCase	yes/no	新規ユーザーに小文字のカレンダを作成するかどうかを指定します。また、カレンダを検索する場合は、小文字のカレンダを検索するかどうかを指定します。
filterPrivateEvents	yes/no	サーバーに照会する場合、プライベートまたは極秘のイベントをフィルタリングするかどうかを指定します。
fbIncludeDefCal	yes/no	ユーザーのデフォルトのカレンダを、そのユーザーの freebusy-calendar-list に含めるかどうかを指定します。
subIncludeDefCal	yes/no	ユーザーのデフォルトカレンダを、そのユーザーの subscribed-calendar-list に含めるかどうかを指定します。
resourceDefaultAcl	yes/no	リソースカレンダにデフォルトの ACL を使用するかどうかを指定します。
calmasterCred	文字列	Calendar Server 管理者として指定されるユーザーの資格。

表 **B–1** `-P` オプションの属性　(続き)

属性	値	説明
`calmasterUid`	文字列	`service.admin.calmaster.userid`
`calmasterAccessOverride`	yes/no	Calendar Server 管理者がアクセス制御を無効にできるかどうかを指定します。
`setPublicRead`	yes/no	デフォルトのユーザーカレンダを公開読み取りか非公開書き込みに設定します。no を選択した場合、ユーザーカレンダが非公開読み取りまたは非公開書き込みに設定されます。
`uiBaseUrl`	文字列	ベースサーバーアドレス。例: `https://proxyserver/`
`uiConfigFile`	文字列	ユーザーインタフェースの設定ファイル。
`uiProxyUrl`	文字列	HTML ユーザーインタフェースの JavaScript ファイルで追加するプロキシサーバーアドレス。例: `https://web_portal.iplanet.com/`
`domainAccess`	文字列	ドメインのアクセス制御文字列。ドメインの相互検索に使用されます。
`uiAllowAnyone`	yes/no	HTML ユーザーインタフェースで、"`Everybody`" ACL の表示および使用を許可するかどうかを指定します。
`allowProxyLogin`	yes/no	プロキシログインを許可するかどうかを指定します。

表 B–2 に示す属性は、次のコマンドで `-R` オプションとともに使用できます。102 ページの「commadmin domain create」 と 107 ページの「commadmin domain modify」 です。属性はビット対応型の値をとります。

WCAP と WCAP の `set-userprefs` コマンドの詳細については、『*Sun Java System Calendar Server Programmer's Manual*』を参照してください。

表 **B–2** `-R` オプションの属性

属性	値	説明
`allowUserDoubleBook`	bit 8	このカレンダを同じタイムスロットで複数回スケジューリングするのを許可します。
`allowResourceDoubleBook`	bit 9	このリソースカレンダを同じタイムスロットで複数回スケジューリングするのを許可します。

表 **B–2** -R オプションの属性　(続き)

属性	値	説明
allowModifyUserPreferences	bit 4	Calendar Server 管理者の get/set userprefs をユーザーの WCAP から取得するのを許可します。
allowModifyPassword	bit 5	ユーザーがサーバー経由でパスワードを変更するのを許可します。
allowCalendarCreation	bit 0	カレンダの作成を許可します。
allowCalendarDeletion	bit 1	カレンダの削除を許可します。
allowPublicWritableCalendars	bit 2	ユーザーに対して公開書き込みが可能なカレンダを保有するのを許可します。
allowSetCn	bit 10	set-userprefs.wcap を使用してユーザー設定 cn を変更するのを許可します。
allowSetGivenName	bit 11	set_userprefs.wcap を使用してユーザー設定 givenname を変更するのを許可します。
allowSetGivenMail	bit 12	set_userprefs.wcap を使用してユーザー設定 mail を変更するのを許可します。
allowSetPrefLang	bit 13	set_userprefs.wcap を使用してユーザー設定 preferredlanguage を変更するのを許可します。
allowSetSn	bit 14	set-userprefs.wcap を使用してユーザー設定 sn を変更するのを許可します。

カレンダタイムゾーン文字列

次のタイムゾーン文字列は、102 ページの「commadmin domain create」、107 ページの「commadmin domain modify」、122 ページの「commadmin resource create」、127 ページの「commadmin resource modify」、130 ページの「commadmin user create」、および 135 ページの「commadmin user modify」 の各コマンドの -T タイムゾーンオプションとともに使用できます。

新しいタイムゾーンを追加し、それをデフォルトのタイムゾーンとして設定することもできます。詳細については、92 ページの「新規カレンダタイムゾーンの追加」を参照してください。

- Africa/Cairo

- Africa/Casablanca
- Africa/Johannesburg
- Africa/Lagos
- Africa/Tripoli
- Africa/Windhoek
- America/Adak
- America/Anchorage
- America/Buenos_Aires
- America/Caracas
- America/Chicago
- America/Costa_Rica
- America/Cuiaba
- America/Denver
- America/Godthab
- America/Grand_Turk
- America/Halifax
- America/Havana
- America/Indianapolis
- America/Los_Angeles
- America/Miquelon
- America/New_York
- America/Phoenix
- America/Port-au-Prince
- America/Santiago
- America/Sao_Paulo
- America/St_Johns
- Asia/Alma-Ata
- Asia/Amman
- Asia/Anadyr
- Asia/Aqtau
- Asia/Aqtobe
- Asia/Baku
- Asia/Bangkok
- Asia/Beirut
- Asia/Bishkek
- Asia/Calcutta
- Asia/Dacca
- Asia/Irkutsk
- Asia/Jerusalem
- Asia/Kabul
- Asia/Kamchatka
- Asia/Karachi
- Asia/Katmandu
- Asia/Krasnoyarsk
- Asia/Magadan
- Asia/Novosibirsk
- Asia/Rangoon
- Asia/Riyadh

- Asia/Shanghai
- Asia/Tokyo
- Asia/Ulan_Bator
- Asia/Vladivostok
- Asia/Yakutsk
- Asia/Yekaterinburg
- Asia/Yerevan
- Atlantic/Azores
- Atlantic/Cape_Verde
- Atlantic/South_Georgia
- Atlantic/Stanley
- Australia/Adelaide
- Australia/Brisbane
- Australia/Darwin
- Australia/Hobart
- Australia/Lord_Howe
- Australia/Sydney
- Europe/Bucharest
- Europe/Istanbul
- Europe/London
- Europe/Minsk
- Europe/Moscow
- Europe/Paris
- Europe/Riga
- Europe/Samara
- Europe/Simferopol
- Europe/Warsaw
- Pacific/Apia
- Pacific/Auckland
- Pacific/Chatham
- Pacific/Easter
- Pacific/Fiji
- Pacific/Gambier
- Pacific/Guadalcanal
- Pacific/Honolulu
- Pacific/Kiritimati
- Pacific/Marquesas
- Pacific/Norfolk
- Pacific/Noumea
- Pacific/Pitcairn
- Pacific/Rarotonga
- Pacific/Tongatapu

付録 C

Delegated Administrator のデバッグ

Delegated Administrator のログ情報は、Delegated Administrator コンポーネント、Delegated Administrator が配備された Web コンテナ、Directory ServerおよびAccess Managerによって生成されたログファイルを検証することによって得られます。

この付録では次の項目について説明します。

コマンド行ユーティリティのデバッグ

Delegated Administrator ユーティリティ (`commadmin`) をデバッグするには、`commadmin` コマンドの `-v` オプションを使ってクライアントのデバッグメッセージを印字します。

Delegated Administrator コンソールログ

Delegated Administrator コンソールは、次の実行時ログファイルを作成します。

- デフォルトログファイル名: `da.log`
- デフォルトの場所: `/opt/SUNWcomm/log`

ログプロパティーファイルを編集すると、独自のログファイルを指定できます。

- ログプロパティーファイル名: `logger.properties`
- デフォルトの場所:

```
/var/opt/SUNWcomm/da/WEB-INF/classes/com/sun/ \
comm/da/resources
```

logger.properties ファイルで次のプロパティを変更できます。

- `da.logging.enable=yes` または `no`

  `yes` を選択するとロギングが有効になり、`no` を選択するとロギングが無効になります。

  デフォルトでは、ロギングは無効です。ロギングを有効にするには、この値を `yes` に設定する必要があります。
- `da.log.file=`*full pathname*

  ロギング文が書き込まれるディレクトリとファイルを指定します。このプロパティにより、`da.log` が指定したファイル名およびファイル位置に変わります。

Delegated Administrator サーバーログ

Web コンテナにインストールされている Delegated Administrator サーブレットによって生成されたデバッグ文を含む Delegated Administrator サーバーログを作成することができます。

これは、Delegated Administrator サーブレットからのデバッグメッセージを Debug サーブレットで記録することによって行います。ブラウザで次の URL に進むと、Debug サーブレットを有効にできます。

`http://`*machine name*`:`*port*`/commcli/debug?op=set&state=all&package=all&filename=`*full path*

各表記の意味は次のとおりです。

- *machine name* は、Delegated Administrator サーバーが起動しているマシンの名前です。
- *full path* は、メッセージが書き込まれるログの名前とフルディレクトリパスです。

例 :

```
http://abc.red.iplanet.com:8008/commcli/debug?op= \
set&state=all&package=all&filename=/tmp/debug.log
```

上記の URL は、Debug サーブレットのメッセージを次のパスにあるファイルに記録します。

```
/tmp/debug.log
```

Webコンテナを再起動したときは、そのつど Debug サーブレットを有効にする必要があります。

Web コンテナサーバーログ

Web コンテナによって生成されるサーバーログを検証すると、Delegated Administrator のデバッグが詳細に行えます。

Web Server

Web Server は、次のパスにアクセスログとエラーログを保持しています。

/web_server_base/`https-`*machine name*/`logs`

各表記の意味は次のとおりです。

- *web_server_base* は、Web Server ソフトウェアがインストールされているパスです。
- *machine name* は、Web Server が起動しているマシンの名前です。

Application Server 7.*x*

Application Server 7.*x* は、次のパスにアクセスログとエラーログを保持しています。

/application_server7_base/`domains/domain1/server1/logs`

各表記の意味は次のとおりです。

- *application_server7_base* は、Application Server 7.*x* ソフトウェアがインストールされているパスです。

Application Server 8.*x*

Application Server 8.*x* は、次のパスにアクセスログとエラーログを保持しています。

サーバーログ:

/application_server8_base/`domains/domain1/logs`

アクセスログ:

/application_server8_base/domains/domain1/logs/access/server_access_log

各表記の意味は次のとおりです。

- *application_server8_base* は、Application Server 8.*x* ソフトウェアがインストールされているパスです。

Directory Server と Access Manager ログ

Directory Server と Access Manager によって生成されるログを検証すると、Delegated Administrator のデバッグが詳細に行えます。

Directory Server

Directory Server は、次のパスにアクセスログとエラーログを保持しています。

/var/opt/mps/serverroot/slapd-*hostname* /logs

各表記の意味は次のとおりです。

- *hostname* は、Directory Server が起動しているマシンの名前です。

Access Manager

Access Manager は、次のパスにログファイルを保持しています。

/var/opt/SUNWam/debug

前述のパスには、amProfile と amAuth ログが含まれています。

/var/opt/SUNWam/logs

前述のパスには、amAdmin.access と amAdmin.error ログが含まれています。

付録 D

Delegated Administrator のパフォーマンスチューニング

次の各項では、Delegated Administrator のパフォーマンスを向上させるための Delegated Administrator と関連ソフトウェアの調整方法を説明します。

この付録で説明するガイドラインに加えて、ディレクトリの中で ACI の統合とデフォルト ACI 数の削減を行うことで、Directory Server のパフォーマンスを向上させることができます。詳細については、付録 E を参照してください。

ユーザー、グループ、および組織の表示速度の向上

組織に多数のユーザーが含まれる場合、Delegated Administrator コンソールの「ユーザー」リストページの表示に時間がかかることがあります。このページで既存のユーザーを読み込み中にユーザーの作成や編集を行おうとすると、エラーが発生します。ページが完全に表示されるまで、いずれのボタンやリンクもクリックしないでください。

同様に、ディレクトリに多数の組織やグループが含まれる場合も、「組織」ページや「グループ」ページの表示に時間がかかることがあります。

これらのページで読み込みに時間がかかる場合、ワイルドカード検索のプロパティーを十分小さい値に設定することで、ページの読み込み速度を向上させることができます。

これらのプロパティーは、次のとおりです。

jdapi-wildusersearchmaxresults　　ユーザーの検索プロパティー。

jdapi-groupsmaxsearchresults　　グループの検索プロパティー。

jdapi-wildorgsearchmaxresults　　組織の検索プロパティー。

ワイルドカード検索プロパティーには次の制限があります。

`-1`　　すべての結果を返します。(すべてのユーザー、グループ、組織を表示。) `-1` はデフォルト値です。

`0`　　検索を行いません。(ユーザー、グループ、組織を非表示。)

n（`>0`）　　*n* 個の結果 (指定された数の結果) を返します。

▼ 「ユーザー」ページの表示速度を向上させる

手順　**1.** **`resource.properties`** ファイルを開きます。

`resource.properties` ファイルは、次のディレクトリにあります。

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **`jdapi-wildusersearchmaxresults`** を低い値に設定します。次に例を示します。

```
jdapi-wildusersearchmaxresults=50
```

または、値を `0` に設定してユーザーを非表示にします。Delegated Administrator コンソールで、「検索」ドロップダウンリストを使用して、指定されたユーザーを検索します。

▼ 「グループ」ページの表示速度を向上させる

手順　**1.** **`resource.properties`** ファイルを開きます。

`resource.properties` ファイルは、次のディレクトリにあります。

da_base`/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties`

2. **`jdapi-groupsmaxsearchresults`** を低い値に設定します。次に例を示します。

```
jdapi-groupsmaxsearchresults=50
```

または、値を `0` に設定してグループを非表示にします。Delegated Administrator コンソールで、「検索」ドロップダウンリストを使用して、指定されたグループを検索します。

▼ 「組織」ページの表示速度を向上させる

手順 1. **resource.properties** ファイルを開きます。

resource.properties ファイルは、次のディレクトリにあります。

da_base/data/WEB-INF/classes/sun/comm/cli/server/servlet/resource.properties

2. **jdapi-wildorgsearchmaxresults** を小さい値に設定します。次に例を示します。

```
jdapi-wildusersearchmaxresults=10
```

または、値を 0 に設定して組織を非表示にします。Delegated Administrator コンソールで、「検索」ドロップダウンリストを使用して、指定された組織を検索します。

JVM ヒープサイズの増加

ページの表示や検索の実行など、Delegated Administrator の一般的な機能のパフォーマンスを向上させるには、Delegated Administrator を配備した Web コンテナが使用する Java 仮想マシン (JVM) のヒープサイズを増加します。Web コンテナの JVM ヒープサイズが小さすぎると、パフォーマンスに影響を及ぼすことがあります。

JVM ヒープサイズは、次の JVM オプションで設定されます。

-Xmx<*n*>m

<*n*> はメガバイト単位のヒープサイズです。

通常、<*n*> は 256m に設定されます。

次の作業は、Web Server と Application Server の JVM ヒープサイズを増加する方法の概要を示します。

▼ Web Server JVM ヒープサイズを増加する

手順 1. **Web Server** 管理サーバーにログインします。

2. 「**Java**」タブの下で、「**JVM Options**」を選択します。

3. **`-Xmx256m`** オプションを編集します。
   このオプションによって JVM ヒープサイズが設定されます。

4. **`-Xmx256m`** オプションの値を大きくします **(`Xmx1024m` など)**。

5. 新しい設定を保存します。

参考 Web Server のマニュアル

Web Server 管理サーバーの使用方法と JVM オプションの設定方法については、『Sun Java System Web Server Administration Guide』および『 Web Server Performance Tuning, Sizing, and Scaling Guide』を参照してください。

▼ Application Server JVM ヒープサイズを増加する

手順 1. **Application Server** 管理サーバーにログインします。

2. **JVM** オプションを表示します。

3. **`-Xmx256m`** オプションを編集します。
   このオプションによって JVM ヒープサイズが設定されます。

4. **`-Xmx256m`** オプションの値を大きくします **(`Xmx1024m` など)**。

5. 新しい設定を保存します。

参考 Application Server のマニュアル

Application Server 管理サーバーの詳細と JVM オプションの設定方法については、『Sun Java System Application Server Documentation Center』の「JVM Advanced Settings」を選択してください。または、『Sun Java System Application Server Enterprise Edition 8.1 2005Q4 Performance Tuning Guide』の「Tuning the Java Runtime System」を参照してください。

Directory Server インデックスしきい値の増加

ユーザーの検索や表示などの Delegated Administrator 機能のパフォーマンスを向上するには、ディレクトリの検索時に Directory Server が使用するインデックスのしきい値を大きくします。

Directory Server が大量の LDAP オブジェクトを検索するときにしきい値が小さいと、検索の完了前にインデックスの領域が不足することがあります。残りの検索はインデックスなしで実行されるので、検索処理が遅くなります。

注意 – この操作は経験豊かな Directory Server 管理者だけが行ってください。

インデックスしきい値を大きく設定するには、`dse.ldif` ファイルの`nssldap-allidsthreshold` オプションの値を変更します。

通常、このオプションの値は次のように設定されています。

```
nssldap-allidsthreshold: 4000
```

`nssldap-allidsthreshold` の値を大きく設定します。次に例を示します。

```
nssldap-allidsthreshold: 200000
```

インデックスしきい値の詳細については、『Sun Java System Directory Server 管理ガイド』の「ディレクトリデータのインデックス作成」の「インデックスの管理」を参照してください。`nssldap-allidsthreshold` オプションの定義については、『Sun Java System Directory Server Administration Reference』の「Server Configuration Reference」の「Database Configuration Attributes」を参照してください。

付録 E

Directory Server パフォーマンスのための ACI 統合

この付録では次の項目について説明します。

はじめに

Messaging Server と Access Manager をインストールして、LDAP Schema 2 ディレクトリを使用すると、数多くの ACI (アクセス制御命令) がディレクトリにインストールされます。デフォルトの ACI の多くは Messaging Server では使用しません。

実行時の ACI をチェックするのは、これが Directory Server のパフォーマンスに影響するためで、結果として Massaging Server のルックアップ操作などのディレクトリ操作のパフォーマンスに影響を与えるからです。

ディレクトリのデフォルト ACI の数を減らしたり統合したりすると、Directory Server のパフォーマンスが向上します。また、ACI を統合すると、管理しやすくなります。

ACI の数を減らす手法は次のとおりです。

- ACI を結合、最適化、および簡素化する
- ACI を修正して、より簡素で効率のよい構文を使用する
- ACI を、ルートサフィックスでほかの ACI と統合する
- 使用していない ACI を削除する
- 多くの組織を持つディレクトリでは、個々の組織ノードで ACI を削除できます。

この付録では、まず ldif ファイル (replacement.acis.ldif) を使用してルートサフィックスで ACI を統合し、使用していない ACI をディレクトリから削除する方法を説明します。詳細については、後述の 182 ページの「ACI の統合と削除」を参照してください。

次にこの付録では各 ACI を分析し、ACI を扱う方法、すなわち削除、変更による効率化、および書き換えの各方法に関する推奨事項を説明します。

ただし、これらの方法は次の条件を前提としています。

- エンドユーザーが Directory コンソールにアクセスしないこと
- エンドユーザーが Access Manager コンソールにアクセスしないこと

この条件を前提にして、ユーザーのインストールの要件に応じて、ldif ファイルを使用して ACI の統合や削除を行うか、または特定の ACI をそのままディレクトリに保持するかを判断する必要があります。

詳細については、この付録で後述する 187 ページの「既存の ACI の分析」を参照してください。

その次に、replacement.acis.ldif ファイルで統合される ACI について説明します。ここでは、統合する前の既存の ACI と、統合されたあとの ACI を示します。詳細については、この付録で後述する 203 ページの「統合した ACI の分析」を参照してください。

最後に、replacement.acis.ldif ファイルで破棄した ACI を示します。詳細については、この付録で後述する 210 ページの「使用せずに破棄する ACI のリスト」を参照してください。

ACI の統合と削除

この項に示した ldif ファイル replacement.acis.ldif は統合した ACI をルートサフィックスにインストールし、使用していない ACI をディレクトリから削除します。Delegated Administrator が提供するこの ldif ファイルは、次のディレクトリにあります。

da_base/lib/config-templates

ldapmodify コマンドを実行して replacement.acis.ldif ファイルをディレクトリに適用すると、ルートサフィックスにある aci 属性のすべてのインスタンスが削除され、replacement.acis.ldif ファイルにある ACI と置き換えられます。

このように、処理手順としては、まずルートサフィックスからすべての ACI を削除してから、下記の ACI と置き換えます。ポータルサーバーなど、ほかのアプリケーションによって生成された ACI がディレクトリに含まれている場合は、その ACI を別のファイルに保存しておき、replacement.acis.ldif ファイルを適用したあとに再度追加します。

この ldif ファイルを使用して ACI を整理する手順については、185 ページの「ACI を置き換える手順」を参照してください。

replacement.acis.ldif File

```
dn: $rootSuffix
changetype: modify
replace: aci
aci: (targetattr = "*")(version 3.0; acl "Configuration Administrator";
   allow (all)
   userdn="ldap:///uid=admin,ou=Administrators,ou=TopologyManagement,
o=NetscapeRoot";)
aci: (target="ldap:///$rootSuffix")
  (targetfilter=(!(objectclass=sunServiceComponent)))
  (targetattr != "userPassword||passwordHistory
   ||passwordExpirationTime||passwordExpWarned||passwordRetryCount
  ||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
  (version 3.0; acl "anonymous access rights";
   allow (read,search,compare)
   userdn = "ldap:///anyone"; )
aci: (targetattr != "nsroledn||aci||nsLookThroughLimit||nsSizeLimit
  ||nsTimeLimit||nsIdleTimeout||passwordPolicySubentry||passwordExpiration
    Time
  ||passwordExpWarned||passwordRetryCount||retryCountResetTime
  ||accountUnlockTime||passwordHistory||passwordAllowChangeTime||uid||mem
    berOf
  ||objectclass||inetuserstatus||ou||owner||mail||mailuserstatus
  ||memberOfManagedGroup||mailQuota||mailMsgQuota||mailhost
  ||mailAllowedServiceAccess||inetCOS||mailSMTPSubmitChannel")
  (version 3.0; acl "Allow self entry modification";
  allow (write)
  userdn ="ldap:///self";)
aci: (targetattr != " aci || nsLookThroughLimit || nsSizeLimit
  || nsTimeLimit|| nsIdleTimeout")
  (version 3.0; acl "Allow self entry read search";
  allow(write)
  userdn ="ldap:///self";)
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Proxy user rights";
  allow (proxy)
  userdn = "ldap:///cn=puser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS special dsame user rights for all under the root
   suffix";
  allow (all)
  userdn = "ldap:///cn=dsameuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
```

```
  (version 3.0; acl "S1IS special ldap auth user rights";
  allow (read,search)
  userdn = "ldap:///cn=amldapuser,ou=DSAME Users,
  $rootSuffix"; )
aci: (target="ldap:///$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Top-level admin rights";
  allow (all)
  roledn = "ldap:///cn=Top-level Admin Role,
  $rootSuffix"; )
aci: (targetattr="*")
  (version 3.0; acl "Messaging Server End User Administrator Read Only
   Access";
  allow (read,search)
  groupdn="ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr="objectclass || mailalternateaddress || Mailautoreplymode
    || mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
    || mailforwardingaddress || mailAutoReplyTimeout
    || mailautoreplytextinternal
    || mailautoreplytext || vacationEndDate || vacationStartDate
    || mailautoreplysubject || maxPabEntries || mailMessageStore
    || mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
    || sunUCTimeFormat || mailuserstatus || maildomainstatus")
  (version 3.0; acl "Messaging Server End User Administrator All Access";
  allow (all)
  groupdn = "ldap:///cn=Messaging End User Administrators Group,ou=Groups,
  $rootSuffix";)
aci: (targetattr = "*")
  (version 3.0;acl "Allow Read-Only Access";
  allow (read,search,compare)
  groupdn = "ldap:///cn=Read-Only,ou=Groups,
  $rootSuffix";)
aci: (target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "S1IS Organization Admin Role access deny";
  deny (write,add,delete,compare,proxy)
  roledn = "ldap:///cn=Organization Admin Role,($dn),
  $rootSuffix";)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetattr="*")
  (version 3.0; acl "Organization Admin Role access allow read";
  allow(read,search)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix" ;)
aci: (target="ldap:///($dn),$rootSuffix")
  (targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
  (entrydn=($dn),$rootSuffix))))
  ( targetattr = "*")
  (version 3.0; acl "S1IS Organization Admin Role access allow";
  allow (all)
  roledn = "ldap:///cn=Organization Admin Role,[$dn],
  $rootSuffix";)
```

ACI を置き換える手順

始める前に

この手順を開始する前に、ディレクトリにある ACI を確認してください。この処理によって削除される ACI の中に、必要なものがないかどうかを調べる必要があるためです。

この手順では、まずすべての ACI をルートサフィックスから削除して、以下に示されている ACI に置き換えます。Massaging Server 以外のアプリケーションによって生成された ACI がディレクトリに含まれている場合は、その ACI を別のファイルに保存しておき、`replacement.acis.ldif` ファイルを適用したあとに再度追加します。

Access Manager と Messaging Server によって生成された既存の ACI を分析する方法については、この付録の後半にある次の項を参照してください。

- 187 ページの「既存の ACI の分析」
- 203 ページの「統合した ACI の分析」
- 210 ページの「使用せずに破棄する ACI のリスト」

ACI の置き換え

次の手順に従って、ルートサフィックスの ACI を統合し、使用していない ACI を削除します。

▼ ACI を置き換える

手順 **1.** ルートサフィックスにある既存の **ACI** を保存します。

これは、次の例のように、`ldapsearch` コマンドを使って行います。

```
ldapsearch -D “cn=Directory Manager” -w <password> -s base -b
<$rootSuffix> aci=* aci ><filename>
```

各表記の意味は次のとおりです。

`<directory manager>` は、Directory Server 管理者のパスワードです。

`<$rootSuffix>` は、ルートサフィックスです (`o=usergroup` など)。

`<filename>` は、保存された ACI が書き込まれるファイルの名前です。

2. **`replacement.acis.ldif`** ファイルをコピーし、名前を変更します。

Delegated Administrator をインストールすると、`replacement.acis.ldif` ファイルが次のディレクトリにインストールされます。

da_base /lib/config-templates

3. **replacement.acis.ldif** ファイルのコピーの **$rootSuffix** エントリを編集します。

   ルートサフィックスのパラメータ $rootSuffix をユーザーのルートサフィックス (o=usergroup など) に変更します。$rootSuffix パラメータは ldif ファイルの中に繰り返し現れるので、必ずすべてのインスタンスを置き換えてください。

4. **LDAP** ディレクトリツール **ldapmodify** を使用して、**ACI** を置き換えます。

   コマンド実行の例を次に示します。

   ```
   ldapmodify -D <directory manager> -w <password> -f
   <replacement.acis.finished.ldif>
   ```

   各表記の意味は次のとおりです。

   <directory manager> は Directory Server 管理者の名前です。

   <password> は、Directory Service 管理者のパスワードです。

   <replacement.acis.finished.ldif> は、ディレクトリ内で ACI の統合と削除を行うための編集済み ldif ファイルの名前です。

動的組織 ACI の削除

Delegated Administrator コンソールで 1 つの組織を作成すると、その組織ノードに ACI のグループが 1 つ作成されます。

前述のとおり ACI を置き換えると、こうした組織ごとの ACI は不要になります。この場合は、Access Manager コンソールを使用して、組織ごとに ACI が作成されないようにします。

▼ 動的組織 ACI を削除する

手順 1. **amadmin** として **AM** コンソールにログインします。

   AM コンソールは、次の URL にあります。

   http://< *machine name*>:<*port* >/amconsole

   各表記の意味は次のとおりです。

   <*machine name*> は、Access Manager を実行しているマシンです。

   <*port*> は、ポートです。

2. 「サービス設定」タブを選択します。

   デフォルトでは、「管理」設定ページが表示されます。

3. コンソールの右側をスクロールダウンして、「ダイナミック管理ロール **ACI**」を表示します。

4. 「ダイナミック管理ロール **ACI**」のテキストボックスの中にあるすべての **ACI** を選択して、削除します。

5. 変更した設定を保存します。

既存の ACI の分析

この項のリストは、Access Manager と Messaging Server をインストールしたときにディレクトリにインストールされる ACI を示しています。また、各 ACI の機能を説明しながら、その ACI を保持、統合、または破棄すべきかを推奨します。

ACI は、次のとおり分類します。

Root Suffix

```
---------------------------------------------------------------------------------------------------

dn: $rootSuffix
#
# consolidate
#
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry
|| passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy state
```

```
attributes";
allow (write)
userdn ="ldap:///self";)
```

アクション: 統合。

このサフィックスへ自己アクセスするための要件はありません。この ACI は重複しています。 ルートサフィックスの自己 ACI に組み込むことができます。

```
#
# retain
#
aci:
(targetattr = "*")
(version 3.0; acl "Configuration Administrator";
allow (all)
userdn = "ldap:///uid=admin, ou=Administrators,
ou=TopologyManagement,o=NetscapeRoot";)
```

アクション: 保持。

`slapd-config` インスタンスへのパススルー認証により認証を行う admin ユーザーです。すべての設定をディレクトリマネージャーとしてコマンド行ユーティリティーで行う場合、この ACI は必要ありません。この資格でコンソールへの認証を行う場合は、この ACI を保持します。同様の ACI は削除してもかまいません。

```
#
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
ou=TopologyManagement, o=NetscapeRoot");)
```

アクション: すべての DB バックエンドで破棄。

委任サーバー管理者特権でコンソールが使用された場合に特権を持つ「設定管理者」グループです。

```
#
# discard
```

```
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)
```

アクション: すべての DB バックエンドで破棄。

一般的な「ディレクトリ管理者」グループの特権の定義です。

```
#
# discard
#
aci:
(targetattr = “*”)
(version 3.0; acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server,
cn=Server Group, cn=whater.red.iplanet.com, ou=red.iplanet.com,
o=NetscapeRoot”;)
```

アクション: すべての DB バックエンドで破棄。

コンソール/管理サーバー関連グループの特権の定義です。

Access Manager

```
# retain
#
aci:
(target=”ldap:///$rootSuffix”)
(targetattr=”*”)
(version 3.0; acl “S1IS Proxy user rights”;
allow (proxy)
userdn = “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”; )
```

アクション: 保持。

この ACI は、システムユーザーの Access Manager へのアクセスを付与します。

```
#
# retain
```

```
#
aci:
 (target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS special dsame user rights for all under the
root suffix";
allow (all)
userdn = "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix"; )
```

アクション: 保持。

この ACI は、システムユーザーの Access Manager へのアクセスを付与します。

```
#
# retain
#
aci:
(target="ldap:///$rootSuffix")(targetattr="*")|
(version 3.0;acl "S1IS special ldap auth user rights";
allow (read,search)
userdn = "ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix"; )
```

アクション: 保持。

この ACI は、システムユーザーの Access Manager へのアクセスを付与します。

```
#
# discard
#
aci:
(target="ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix")
(targetattr = "*")
(version 3.0;
acl "S1IS special ldap auth user modify right";
deny (write)
roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、最上位管理者 (TLA) によって amldapuser アカウントが変更されるのを防ぎます。

```
#
# retain
```

```
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin rights";
allow (all)
roledn = "ldap:///cn=Top-level Admin Role,$rootSuffix"; )
```

アクション: 保持。

この ACI は、最上位管理者のロールへのアクセスを付与します。

```
#
# discard
#
aci:
(targetattr="iplanet-am-saml-user || iplanet-am-saml-password")
(targetfilter="(objectclass=iplanet-am-saml-service)")
(version 3.0; acl "S1IS Right to modify saml user and password";
deny (all)
(roledn != "ldap:///cn=Top-level Admin Role,$rootSuffix")
AND (userdn != "ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix")
AND (userdn != "ldap:///cn=puser,ou=DSAME Users,$rootSuffix"); )
```

アクション: 破棄。

この ACI は、SAML関連の属性を保護します。

Top-level Help Desk Admin Role

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

アクション: 破棄。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

アクション: 破棄。

Top-level Policy Admin Role

```
#
# discard
#
aci:
target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Top-level Policy Admin のロールに関係しています。

```
#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access Auth Service
deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Top-level Policy Admin のロールに関係しています。

```
#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Top-level Policy Admin のロールに関係しています。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Top-level Policy Admin のロールに関係しています。

AM Self

```
#
# consolidate
#
aci:
(targetattr = "*")
(version 3.0;
acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)
```

アクション: 1つの自己書き込み ACI に統合。エンドユーザーは、自分自身を含めて、エントリを削除する権限を持っていないので、明示的な拒否を行う必要はありません。

これは、自己特権を設定する ACI の 1 つです。明示的な拒否を行うと、エントリがそれ自体を削除することを防げます。

```
#
# consolidate
#
aci:
(targetattr = "objectclass || inetuserstatus
|| iplanet-am-user-login-status
|| iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || iplanet-am-user-account-life
|| iplanet-am-session-max-session-time || iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)
```

アクション: 1つの自己書き込み ACI に統合。

これは、自己書き込み特権を設定する ACI の 1 つです。

```
#
# consolidate
#
aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| nsLookThroughLimit || nsSizeLimit || nsTimeLimit || nsIdleTimeout
|| memberOf || iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except for nsroledn,
aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)
```

アクション: 1つの自己書き込み ACI に統合。

これは、特権を設定する ACI の 1 つです。

```
#
# consolidate
#
aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for nsroledn,
aci, resource limit and web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)
```

アクション: 1つの自己書き込み ACI に統合。

これは、自己書き込み特権を設定する ACI の 1 つです。

AM Anonymous

```
#
# consolidate
#
aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

アクション: 1つの匿名 ACI に統合。

これは、匿名の特権を与える ACI の 1 つです。

```
#
# consolidate
#
aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

アクション: 1つの匿名 ACI に統合。

これは、匿名の特権を与える ACI の 1 つです。

```
-----------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------

#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )
```

アクション: 破棄。

この ACI は、デフォルト組織がユーザー (rootdn を除く) によって削除されることを防ぎます。

```
-----------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------

#
# discard
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

アクション: 破棄。

この ACI は、最上位管理者のロールがユーザー (rootdn を除く) によって削除されることを防ぎます。

```
-----------------------------------------------------------------------------------------------
```

AM Deny Write Access

```
-----------------------------------------------------------------------------------------------

#
# discard
#
aci: (targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Deny Write Access Role に関係しています。

AM Container Admin Role

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)
```

アクション: 破棄。

この ACI は、Container Admin Role に関係しています。

```
#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)
```

アクション: 破棄。

この ACI は、Container Admin Role に関係しています。

```
#
# discard
#
aci:
 (target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
```

```
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Group and People Container Admin Role に関係しています。

Organization Help Desk

```
#
# discard
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Organization Help Desk Admin Role に関係しています。

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
```

```
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

アクション: 破棄。

この ACI は、Organization Help Desk Admin Role に関係しています。

AM Organization Admin Role

```
#
# consolidate
#
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

アクション: 統合。

```
#
# consolidate
#
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)
```

アクション: 統合。

この ACI は、Organization Admin Role に関係しています。

```
#
# consolidate
#
aci: (missing)
```

```
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

アクション: 統合。

この ACI は、Organization Admin Role に関係しています。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

アクション: 統合。

この ACI は、Organization Admin Role に関係しています。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox ||
postalCode
|| registeredaddress || street || l || st || telephonenumber
||maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

アクション: 統合。

この ACI は、Organization Admin Role に関係しています。

```
#
# consolidate
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

アクション: 統合。

AM Miscellaneous

```
#
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

アクション: 破棄。

この ACI を破棄すると、属性 `iplanet-am-modifiable-by` に伴う特権が無効になります。

Messaging Server

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
```

```
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

アクション: 統合。

この ACI は、Messaging End User Administrators Group に許可を付与します。

```
#
# consolidate
#
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode
||mailprogramdeliveryinfo||nswmextendeduserprefs||preferredlanguage
||maildeliveryoption||mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext
||vacationEndDate||vacationStartDate||mailautoreplysubject||pabURI
||maxPabEntries||mailMessageStore||mailSieveRuleSource||sunUCDateFormat
||sunUCDateDeLimiter||sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
$rootSuffix";)
```

アクション: 統合。

この ACI は、Messaging End User Administrators Group に許可を付与します。

```
#
# consolidate
#
aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota||inetSubscriberAccountId||dataSource||mailhost
||mailAllowedServiceAcces||pabURI||inetCOS||mailSMTPSubmitChannel
||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization
Admin Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

アクション: 統合。

これは、自己特権を設定する ACI の 1 つです。

統合した ACI の分析

この項では、置換用 ldif ファイル `replacement.acis.ldif` で統合された ACI を示します。 このファイルは、ディレクトリで ACI を統合するために使用します。ACI を置き換える方法については、185 ページの「ACI を置き換える手順」を参照してください。

以下の ACI は、対になっています。分類ごとに、まず元の ACI を、次に統合した ACI を示します。

元の Anonymous Access Rights

```
aci:
(targetattr != "userPassword || passwordHistory || passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordAllowChangeTime ")
(version 3.0; acl "Anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)

aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


aci:
(target="ldap:///$rootSuffix")
```

```
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


aci:
(target="ldap:///ou=services,$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr = "*")
(version 3.0; acl "S1IS Services anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)


aci:
(target="ldap:///ou=iPlanetAMAdminConsoleService,*,$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS iPlanetAMAdminConsoleService anonymous access";
allow (read, search, compare)
userdn = "ldap:///anyone";)
```

統合した Anonymous Access Rights

```
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(objectclass=sunServiceComponent)))
(targetattr != "userPassword||passwordHistory
||passwordExpirationTime||passwordExpWarned||passwordRetryCount
||retryCountResetTime||accountUnlockTime||passwordAllowChangeTime")
(version 3.0; acl "anonymous access rights";
allow (read,search,compare)
userdn = "ldap:///anyone"; )
```

分析: この ACI はルート上にあり、元の匿名 ACI と同様のアクセスを許可します。これは、除外属性をリストすることで行われます。この置換 ACI により、ターゲットから (*) が削除されるため、パフォーマンスが向上します。

元の自己 ACI

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit ||
nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
passwordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime ||
accountUnlockTime || passwordHistory || passwordAllowChangeTime")
(version 3.0; acl "Allow self entry modification except for nsroledn, aci,
resource limit attributes, passwordPolicySubentry and password policy
state attributes";
allow (write)
```

```
userdn ="ldap:///self";)


aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny deleting self";
deny (delete)
userdn ="ldap:///self";)


aci:
(targetattr = "objectclass || inetuserstatus ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list
|| iplanet-am-user-account-life || iplanet-am-session-max-session-time
|| iplanet-am-session-max-idle-time
|| iplanet-am-session-get-valid-sessions
|| iplanet-am-session-destroy-sessions
|| iplanet-am-session-add-session-listener-on-all-sessions
|| iplanet-am-user-admin-start-dn
|| iplanet-am-auth-post-login-process-class")
(targetfilter=(!(nsroledn=cn=Top-levelAdmin Role,$rootSuffix)))
(version 3.0; acl "S1IS User status self modification denied";
deny (write)
userdn ="ldap:///self";)


aci:
(targetattr != "iplanet-am-static-group-dn || uid || nsroledn || aci
|| LookThroughLimit
|| nsSizeLimit || nsTimeLimit || nsIdleTimeout || memberOf ||
planet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow ||
planet-am-web-agent-access-deny-list")
(version 3.0; acl "S1IS Allow self entry modification except
for nsroledn, aci, and resource limit attributes";
allow (write)
userdn ="ldap:///self";)


aci:
(targetattr != "aci || nsLookThroughLimit || nsSizeLimit || nsTimeLimit
|| nsIdleTimeout || iplanet-am-domain-url-access-allow")
(version 3.0; acl "S1IS Allow self entry read search except for
nsroledn, aci, resource limit and web agent policy attributes";
allow (read,search)
userdn ="ldap:///self";)


aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress
||mailEquivalentaddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota
||mailMsgQuota
```

```
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

統合した自己 ACI

```
aci:
(targetattr != "nsroledn || aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit || nsIdleTimeout || passwordPolicySubentry ||
asswordExpirationTime
|| passwordExpWarned || passwordRetryCount || retryCountResetTime
|| accountUnlockTime || passwordHistory || passwordAllowChangeTime ||
id || memberOf
|| objectclass || inetuserstatus || ou || owner || mail || mailuserstatus
|| memberOfManagedGroup ||mailQuota || mailMsgQuota || mailhost
|| mailAllowedServiceAccess || inetCOS || mailSMTPSubmitChannel")
(version 3.0; acl "Allow self entry modification";
allow (write)
userdn ="ldap:///self";)
```

```
aci:
(targetattr != " aci || nsLookThroughLimit || nsSizeLimit
|| nsTimeLimit|| nsIdleTimeout")
(version 3.0; acl "Allow self entry read search";
allow(read,search)
userdn ="ldap:///self";)
```

分析: すべての `iplanet-am-*` 属性が削除されています。ACI が存在しない場合は deny がデフォルトとなるので、すべての deny ACI が削除されています。`write` を許可するものは、1 つの ACI に統合されています。

元の Messaging Server ACI

```
aci:
(target="ldap:///$rootSuffix")
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator Read
Access Rights -
product=SOMS,schema 2 support,class=installer,num=1,version=1";
allow (read,search)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)
```

```
aci:
(target="ldap:///$rootSuffix")
(targetattr="objectclass||mailalternateaddress||mailautoreplymode||
mailprogramdeliveryinfo
||nswmextendeduserprefs||preferredlanguage||maildeliveryoption||
mailforwardingaddress
||mailAutoReplyTimeout||mailautoreplytextinternal||mailautoreplytext||
vacationEndDate
||vacationStartDate||mailautoreplysubject||pabURI||maxPabEntries||
mailMessageStore
||mailSieveRuleSource||sunUCDateFormat||sunUCDateDeLimiter||
sunUCTimeFormat")
(version 3.0; acl "Messaging Server End User Adminstrator Write
Access Rights -
product=SOMS,schema 2 support,class=installer,num=2,version=1";
allow (all)
groupdn="ldap:///cn=Messaging End User Administrators Group, ou=Groups,
rootSuffix";)


aci:
(targetattr="uid||ou||owner||mail||mailAlternateAddress||
mailEquivalentAddress||memberOf
||inetuserstatus||mailuserstatus||memberOfManagedGroup||mailQuota||
mailMsgQuota
||inetSubscriberAccountId||dataSource||mailhost||mailAllowedServiceAccess
||pabURI||inetCOS||mailSMTPSubmitChannel||aci")
(targetfilter=(&(objectClass=inetMailUser)(!(nsroledn=cn=Organization Admin
Role,*))))
(version 3.0; acl "Deny write access to users over Messaging Server
protected attributes -
product=SOMS,schema 2 support,class=installer,num=3,version=1 ";
deny (write)
userdn = "ldap:///self";)
```

統合した Messaging Server ACI

自己 ACI は、自己 ACI の中で取り扱われます。

```
aci:
(targetattr="*")
(version 3.0; acl "Messaging Server End User Administrator
Read Only Access";
allow (read,search)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix"; )


aci:
(targetattr="objectclass || mailalternateaddress || Mailautoreplymode
|| mailprogramdeliveryinfo || preferredlanguage || maildeliveryoption
|| mailforwardingaddress || mailAutoReplyTimeout
|| mailautoreplytextinternal
```

```
|| mailautoreplytext || vacationEndDate || vacationStartDate
|| mailautoreplysubject || maxPabEntries || mailMessageStore
|| mailSieveRuleSource || sunUCDateFormat || sunUCDateDeLimiter
|| sunUCTimeFormat || mailuserstatus || maildomainstatus")
(version 3.0; acl "Messaging Server End User Administrator All Access";
allow (all)
groupdn = "ldap:///cn=Messaging End User Administrators
group,ou=Groups,$rootSuffix";)
```

分析: 元の ACI と同じです。

元の Organization Admin ACI

```
aci: (different name - "allow all" instead of "allow")
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn ="ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)


aci: (missing)
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read to org node";
allow (read,search)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr!="businessCategory || description || facsimileTelephoneNumber
|| postalAddress || preferredLanguage || searchGuide || postOfficeBox
|| postalCode
|| registeredaddress || street || l || st || telephonenumber
|| maildomainreportaddress
|| maildomainwelcomemessage || preferredlanguage || sunenablegab")
(version 3.0; acl "Organization Admin Role access deny to org node";
deny (write,add,delete)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix" ;)
```

```
aci: (duplicate of per organization aci)
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///cn=Organization Admin
Role,($dn),dc=red,dc=iplanet,dc=com")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=red,dc=iplanet,dc=com))))
(targetattr = "nsroledn")
(targattrfilters="add=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,
o=SharedDomainsRoot,o=Business,$rootSuffix),
del=nsroledn:(nsroledn=*,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,
o=Business,$rootSuffix)")
(version 3.0;
acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,o=fullOrg1,o=VIS,o=siroe.com,o=SharedDomainsRoot,o=Business,
$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Organization Admin Role access allow all";
allow (all)
roledn = "ldap:///cn=Organization Admin
Role,[$dn],dc=red,dc=iplanet,dc=com";)
```

統合した Organization Admin ACI

```
aci:
(target="ldap:///cn=Organization Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Organization Admin Role access deny";
```

```
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Organization Admin Role,($dn),$rootSuffix";)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "Organization Admin Role access allow read";
allow(read,search)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix" ;)


aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(entrydn=($dn),$rootSuffix))))
( targetattr = "*")
(version 3.0; acl "S1IS Organization Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Organization Admin Role,[$dn],$rootSuffix";)
```

使用せずに破棄する ACI のリスト

この項のリストは、`replacement.acis.ldif` ファイルをディレクトリに適用したときに、ディレクトリから破棄される未使用のデフォルト ACI を示しています。

破棄されるACI は、次のとおり分類します。

Suffix

```
# discard
#
aci:
(targetattr ="*")
(version 3.0;acl "Configuration Administrators Group";
allow (all)
(groupdn = "ldap:///cn=Configuration Administrators, ou=Groups,
```

```
ou=TopologyManagement, o=NetscapeRoot”);)


#
# discard
#
aci:
(targetattr =”*”)
(version 3.0;acl “Directory Administrators Group”;
allow (all)
(groupdn = “ldap:///cn=Directory Administrators, $rootSuffix”);)


#
# discard
#
aci:
(targetattr = “*”)
(version 3.0;
acl “SIE Group”;
allow (all)
groupdn = “ldap:///cn=slapd-whater, cn=Sun ONE Directory Server, cn=Server
Group, cn=whater.red.iplanet.com, ou=red.iplanet.com, o=NetscapeRoot”;)


#
# discard - prevents TLA from modifying the amldapuser account.
#
aci:
(target=”ldap:///cn=amldapuser,ou=DSAME Users,$rootSuffix”)
(targetattr = “*”)
(version 3.0;
acl “S1IS special ldap auth user modify right”;
deny (write)
roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”;)


#
# discard - protects SAML related attributes
#
aci:
(targetattr=”iplanet-am-saml-user || iplanet-am-saml-password”)
(targetfilter=”(objectclass=iplanet-am-saml-service)”)
(version 3.0; acl “S1IS Right to modify saml user and password”;
deny (all)
(roledn != “ldap:///cn=Top-level Admin Role,$rootSuffix”)
AND (userdn != “ldap:///cn=dsameuser,ou=DSAME Users,$rootSuffix”)
AND (userdn != “ldap:///cn=puser,ou=DSAME Users,$rootSuffix”); )
```

Top-level Help Desk Admin Role

```
#
# discard
 #
```

```
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(nsroledn=cn=Top-level Admin Role,$rootSuffix)))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Top-level Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Top-level Help Desk Admin Role,$rootSuffix";)
```

Top-level Policy Admin Role

```
#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=iPlanetAMAuthService,ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access
Auth Service deny";
deny (add,write,delete)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=services,*$rootSuffix")
(targetattr = "*")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
```

```
allow (all)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter="(objectclass=sunismanagedorganization)")
(targetattr = "sunRegisteredServiceName")
(version 3.0; acl "S1IS Top-level Policy Admin Role access allow";
allow (read,write,search)
roledn = "ldap:///cn=Top-level Policy Admin Role,$rootSuffix";)
```

Access Manager Anonymous

```
#
# discard - prevents anyone other than rootdn from deleting
# default organization.
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(entrydn=$rootSuffix))
(targetattr="*")
(version 3.0; acl "S1IS Default Organization delete right denied";
deny (delete)
userdn = "ldap:///anyone"; )


#
# discard - prevents any user other than rootdn from deleting the
# TLA admin role.
#
aci:
(target="ldap:///cn=Top-level Admin Role,$rootSuffix")
(targetattr="*")
version 3.0; acl "S1IS Top-level admin delete right denied";
deny(delete)
userdn = "ldap:///anyone"; )
```

Access Manager Deny Write Access

```
#
# discard
#
aci:
(targetattr = "*")
(version 3.0; acl "S1IS Deny write to anonymous user";
deny (add,write,delete)
roledn ="ldap:///cn=Deny Write Access,$rootSuffix";)
```

Access Manager Container Admin Role

```
#
# discard
#
aci:
(target="ldap:///($dn),$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix))))
(targetattr != "nsroledn")
(version 3.0; acl "S1IS Container Admin Role access allow";
allow (all)
roledn = "ldap:///cn=Container Admin Role,[$dn],$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///cn=Container Admin Role,($dn),$rootSuffix")
(targetattr="*")
(version 3.0; acl "S1IS Container Admin Role access deny";
deny (write,add,delete,compare,proxy)
roledn = "ldap:///cn=Container Admin Role,($dn),$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///ou=People,$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix)
(nsroledn=cn=Container Admin Role,$rootSuffix))))
(targetattr != "iplanet-am-web-agent-access-allow-list
|| iplanet-am-domain-url-access-allow
|| iplanet-am-web-agent-access-deny-list || nsroledn")
(version 3.0; acl "S1IS Group and people container admin role";
allow (all)
roledn = "ldap:///cn=ou=People_dc=red_dc=iplanet_dc=com,$rootSuffix";)
```

Organization Help Desk

```
#
# discard
#
aci: (extra verses dreambig)
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
```

```
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "*")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (read,search)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)


#
# discard
#
aci:
(target="ldap:///$rootSuffix")
(targetfilter=(!(|(nsroledn=cn=Top-level Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Help Desk Admin Role,$rootSuffix)
(nsroledn=cn=Top-level Policy Admin Role,$rootSuffix)
(nsroledn=cn=Organization Admin Role,$rootSuffix))))
(targetattr = "userPassword")
(version 3.0; acl "S1IS Organization Help Desk Admin Role access allow";
allow (write)
roledn = "ldap:///cn=Organization Help Desk Admin Role,$rootSuffix";)
```

Access Manager Miscellaneous

```
#
# discard - Removal disables the associated privileges to the attribute
# iplanetam-modifiable-by
#
aci:
(target="ldap:///$rootSuffix")
(targetattr!="nsroledn")
(version 3.0; acl "S1IS Group admin's right to the users he creates";
allow (all)
userattr = "iplanet-am-modifiable-by#ROLEDN";)
```

索引

I

J

L

M

N